Escola Politècnica Superior
de Castelldefels
UNIVERSITAT POLITÈCNICA DE CATALUNYA

TRABAJO DE FINAL DE CARRERA

Título: Análisis e implementación tecnológica de la infraestructura de comunicaciones de una empresa logística distribuidora de productos farmacéuticos

Titulación: Ingeniería Técnica de Telecomunicaciones, especialidad Telemática

Autor: Julián Moreno Becerra

Director: Luis G. Alonso Zárate

Fecha: 1 de Abril de 2011

Resum

El mundo que conocemos en la actualidad es un mundo que no para de evolucionar, constantemente surgen mejoras tecnológicas, nuevas técnicas de transmisión de la información, etc. Esta evolución obliga a que todas las empresas tengan que estar renovándose constantemente, ya sea en el ámbito de las comunicaciones, como se menciono anteriormente, u ofreciendo nuevos servicios y mejorando la calidad de los servicios que ya se dan.

Este proyecto describe el proceso de mejora en el sistema de comunicaciones de una empresa logística distribuidora de productos farmacéuticos. Esta empresa tenía unos sistemas informáticos y de comunicaciones obsoletos y en un corto periodo de tiempo ha evolucionado a un estado óptimo.

Inicialmente se describe del tipo de empresa, su funcionamiento y la problemática que existe debido a su actividad laboral, de tal manera que se pueda entender mejor las decisiones y explicaciones que se han ido tomando a lo largo del proyecto.

Posteriormente se realiza un análisis del estado inicial del sistema de comunicaciones de la empresa donde se buscan los puntos débiles de esta: baja calidad en algunas de sus comunicaciones, hardware obsoleto en la mayoría de sus almacenes, falta de sistemas de back-up, etc.

A consecuencia de las carencias encontradas se han propuesto soluciones para solventar estos problemas: aumento de la capacidad de las comunicaciones, renovación de hardware, cambio en la topología de la red, etc.

Una vez estudiadas las soluciones propuestas, las mismas se han ido implementando en los sistemas de comunicaciones de la empresa.

Finalmente, se muestran las mediciones del sistema a partir de las mejoras propuestas y se han extraído resultados en los que se muestra la mejora del rendimiento que han dado dichas modificaciones, no solo en el aspecto técnico, también en el aspecto productivo (aumento en la demanda de pedidos, descenso en el tiempo de procesado de estos,…).

Title: Analysis and technologic implementation of the communication infrastructure of a logistic company that distributed pharmaceutics articles

Author: Julián Moreno Becerra

Director: Luis G. Alonso Zárate

Date: April, 1th 2011

Overview

The world that we know at present does not stop evolving, it constantly arises technological improvements and new transmission technologies, etc. This evolution forces that all the companies have to be renewed constantly, both regarding its communication systems and, as previously mentioned, offering new services and improving the quality of the services that already are given.

This project describes the communications systems improvement process of a logistic distribution company of pharmaceutical products. This company had obsolete IT systems and, in a short period of time, it has managed to settle and to evolve them to an ideal condition.

Firstly, the type of company and its functioning are described; together with the problematic that exists due to its activity, in such a way that the decisions and explanations carried out during the project are properly highlighted.

Then, an initial analysis of the previous state of the company's communications network is shown, and its weak points are identified: low quality in some of its communications, obsolete hardware, lack of back-ups, etc.

As a result, we have proposed solutions to fix these problems, which include an increase of the capacity of the communications, the renovation of hardware, some changes in the topology of the network, etc.

Once described the proposed solutions, they have been actually implemented in the communications systems of the company.

Finally some measurements have been carried out and some extracted results are shown in order to highlight the obtained performance improvement, not only in terms of technical aspects, but also in productive issues (increase of the demand orders, decrease of the processing time…).

Quisiera dedicar este TFC a todo el departamento de Sistemas Informáticos de FDF que tanto me han ayudado en todas las dudas que he tenido, en especial a Santi y a Raúl.

INDICE

1. INTRODUCCIÓN

1.1 Motivación y Objetivos

La progresión tecnológica en la que estamos sumergidos desde inicios del siglo pasado ha acontecido numerosos beneficios para el desarrollo de la humanidad; pero a la vez se obliga a su uso, si no se aprovechan estos beneficios puede desarrollar una serie de problemas.

Esta progresión está pasando factura a muchas empresas (sobretodo las que poseen cierta antigüedad), las cuales se han encontrado con que muchos de sus sistemas se están quedando o se han quedado obsoletos (sistemas de comunicaciones, sistemas informáticos,…). Esto junto a la gran competencia que existe en el mercado, ha llevado a muchas de estas, tomar la decisión de renovarse, o de lo contrario *"morir"*.

Este proyecto consiste en la evolución que se ha acontecido en una empresa con las características comentadas con anterioridad y los pasos que se han ido tomando hasta evolucionar a un estado óptimo tecnológico, el cual se está logrando en la actualidad.

Esta empresa se trata de una distribuidora de productos farmacéuticos que data de principios de siglo XX (de ahora en adelante nos referiremos a esta empresa como FDF).

En la actualidad la sede central y oficinas de FDF se encuentra en la provincia de Barcelona, donde también se encuentra el almacén principal, a parte de este almacén tiene varios almacenes distribuidos por la geografía catalana y valenciana.

El funcionamiento principal en el que se basa FDF consiste en recibir la demanda de artículos farmacéuticos de sus OF a través de servidores de recepción de pedidos. Llamamos OF (oficinas farmacéuticas) a los establecimientos farmacéuticos que gestionan estos pedidos en los cuales proporcionan información en las cabeceras de los pedidos que crean, como por ejemplo qué almacén o en qué turno quieren que se les sirva el pedido.

La problemática que nos encontramos es que existen ciertos factores que pueden impedir que la recepción y la entrega del pedido se realice con éxito. Como consecuencia a esto, es probable que la OF busque realizar su pedido a otro distribuidor, perdiendo de esta manera no solo el pedido, sino la "confianza" de este cliente en futuras ventas.

Por esta razón, el Departamento de Sistemas Informáticos de FDF, del cual formo parte, ha realizado un plan de sistemas para renovar la infraestructura tecnológica y de procesos con el objetivo de renovarse, ser estables y competentes en el mercado y, de esta forma; crecer y obtener la confianza de nuestros clientes.

1.2 Modelo y características de FDF

Existen muchos factores para determinar de qué tipo es una empresa, en función del número de trabajadores que tenga, el sector en el cual se desenvuelva, las funciones que desempeñe, privada o pública, sociedad anónima o colectiva, en fin; una gran variedad.

En este caso nos encontramos que FDF es una *Cooperativa Logística distribuidora de productos farmacéuticos*.

Primero de todo definiremos qué es una cooperativa. Una cooperativa es una empresa que no posee ánimo de lucro y está constituida para satisfacer las necesidades o intereses socioeconómicos de los cooperativistas, quienes también son a la vez trabajadores, y en algunos casos también proveedores y clientes de la empresa.

Su intención es hacer frente a sus necesidades y aspiraciones económicas, sociales y culturales comunes haciendo uso de una empresa. La diversidad de necesidades y aspiraciones (trabajo, consumo, comercialización conjunta, enseñanza, crédito, etc.) de los socios, que conforman el objeto social de estas empresas, define una tipología muy variada de cooperativas.

Otro aspecto a definir es el de empresa distribuidora/comercial. Cuando hacemos referencia a este término nos referimos a empresas que se dedican o realizan el acto propio de la distribución o comercio. Su función principal es la compra-venta de productos terminados en la cual interfieren dos intermediarios que son el productor y el consumidor.

Por otro lado tendríamos que definir el término logístico vinculado bastante con el término anterior. La logística es la acción del colectivo laboral dirigida a garantizar las actividades de diseño y dirección de los flujos material, informativo y financiero, desde sus fuentes de origen hasta sus destinos finales, que deben ejecutarse de forma racional y coordinada con el objetivo de proveer al cliente los productos y servicios en la cantidad, calidad, plazos y lugar demandados con elevada competitividad.

La función logística se encarga de la gestión de:

- Recursos (humanos, consumibles, electricidad…)
- Bienes necesarios a la realización de la prestación (almacenes propios, herramientas, camiones propios, sistemas informáticos…)
- Servicios (transportes o almacén subcontratados, …)

En definitiva, el objetivo de definir FDF como empresa no es otro que darnos cuenta la relación que puedan tener las características que hemos expuesto con las comunicaciones, y de esto nos damos cuenta cuando analizamos el significado de empresa distribuidora, lo cual implica una comunicación entre esta y los consumidores, a mayor calidad de comunicación, mayor rendimiento de la empresa.

1.3 Historia de FDF

La década de los años veinte fue una época difícil para los farmacéuticos. Sufrían fuertes imposiciones de las entidades distribuidoras, las cuales aprovecharon la aparición de las primeras especialidades farmacéuticas para imponer sus propias normas económicas y de distribución. Además, tenían que soportar la competencia desleal de las droguerías, y el colectivo se consideraba discriminado por la Administración, que no reconocía la personalidad y los derechos de la clase farmacéutica.

El 12 de julio de 1928 nace esta cooperativa cuando un grupo de farmacéuticos de Barcelona deciden unirse para poder comprar y después repartirse entre ellos el máximo volumen de partidas de especialidades farmacéuticas que se podían vender más fácilmente y, de esta forma, obtener los máximos descuentos.

Durante la década de los 80 la FDF se centra en reconducir la situación económica, replantear las necesidades de toda la red de almacenes con visión de futuro, modernizar el funcionamiento de la Cooperativa mediante la informática y la robótica, y luchar a fondo y sin tregua para promover el espíritu cooperativista y la unión entre los socios de FDF.

El almacén principal de la empresa en la actualidad, el almacén de Terrassa; se inaugura en diciembre de 1984 con dos objetivos: dar servicio a los socios de Barcelona desde fuera de la ciudad y tener un almacén con espacio para introducir las nuevas tecnologías y usarlo como almacén regulador de los demás.

Anuncio de la época

Empleados de FDF en el almacén de Terrassa

En el transcurso de la década de los 90 los almacenes se adecúan tecnológicamente con la robotización y la radiofrecuencia y se lanza FDFWIN un programa de gestión para las oficinas de OF.

1.4 Funcionamiento de FDF

En este apartado se desea mostrar el funcionamiento que posee FDF, a qué se dedica realmente, de este modo se comprenderá la problemática del sistema y se entenderán mejor las decisiones que se tomen en sus sistemas de comunicaciones.

La sede central de FDF se encontraba ubicada en Barcelona, donde se encontraban sus oficinas (inicialmente también hacía funciones de almacén hasta los años 90) y existían siete sedes más distribuidas entre las comunidades autónomas de Valencia y Cataluña **(Fig.2.1)** que realizaban la función de almacenes donde se preparan los pedidos a las OF. El número de empleados que tenía la empresa era de 446 trabajadores entre oficinas, almacenes y transportistas.

Fig. 2.1 Mapa territorial de las sedes de la empresa en su fase inicial

Para explicar el funcionamiento que posee FDF simularemos los pasos que se deben realizar desde que el farmacéutico socio de FDF solicita un pedido hasta que llega el pedido al establecimiento de nuestro cliente con el material solicitado.

El proceso se inicia cuando un usuario cualquiera se dispone a realizar la compra de ciertos artículos en una OF (oficina farmacéutica).

La OF tiene un stock en el cual puede o no disponer de este artículo, ya sea por falta de existencias o porque es un artículo que al ser tan poco usual nunca dispongan de él. En cualquiera de los dos casos la OF realiza un pedido de los artículos que necesite hacía FDF.

Por otra parte FDF mantiene en sus almacenes un gran stock donde abunda la cantidad y variedad de artículos para poder dotar a las OF que los requieran. FDF realiza compras al fabricante de estos artículos al por mayor obteniendo un precio menor de estos y de esta forma consiguiendo beneficios en ventas posteriores.

Una vez recibido el pedido, FDF lo gestiona y una vez preparado, lo envía a la OF a través del sistema de transportistas que posee.

En la siguiente figura (**Fig. 2.2**) realizamos un diagrama de lo anteriormente explicado:

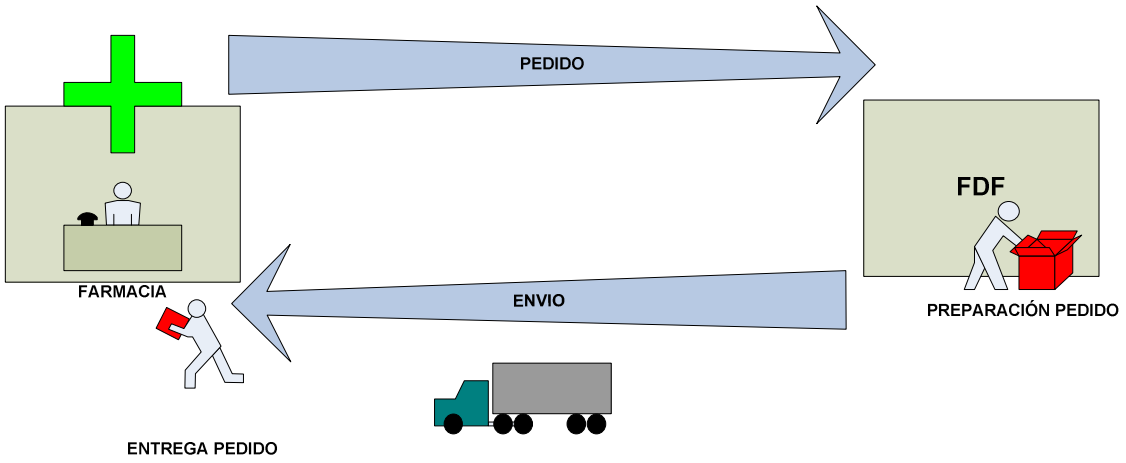


Fig. 2.2 Diagrama de funcionamiento de FDF

Los pedidos se realizan normalmente en tramos horarios durante la jornada laboral del farmacéutico en la cual existe menor carga de trabajo. Normalmente este tramo horario se encuentra de 13h a 14h y de 20h a 21h aproximadamente, horas próximas al cierre de la mayor parte de establecimientos.

Con esta afirmación podemos determinar que el mayor número de pedidos que recibe FDF se efectuarán durante estas horas y que en función de los recursos que se requieran para poder tramitar y gestionar estos pedidos y de esta forma soportar esta carga de trabajo, se deberá dimensionar el sistema de comunicaciones de FDF.

1.5 Comunicaciones empleadas en FDF

A continuación se muestra un repaso teórico de los medios de transmisión que se han empleado en el transcurso del proyecto, y las tecnologías empleadas sobre estos medios, para que posteriormente se pueda entender con más claridad el contenido en siguientes capítulos.

1.5.1 Medios físicos de transmisión empleados

1.5.1.1 Fibra óptica

La fibra óptica se trata de un medio de transmisión que se emplea habitualmente en redes de datos. Se trata de un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían pulsos de luz que representan los datos a transmitir. La fuente de luz puede ser a través de un láser o de un LED. El haz de luz se propaga por el núcleo de la fibra con un ángulo de reflexión por encima del ángulo límite de reflexión total, esto se calcula mediante la ley de *Snell* que muestro a continuación:

$$\eta_1 \operatorname{sen}\theta_1 = \eta_2 \operatorname{sen}\theta_2$$

Las fibras ópticas tienen un uso muy común dentro del mundo de las telecomunicaciones, ya que permiten enviar gran cantidad de datos a una gran distancia, con velocidades similares a las de radio o cable. Son el medio de transmisión por excelencia al ser inmune a las interferencias electromagnéticas, también se utilizan para redes locales, en donde se necesite aprovechar las ventajas de la fibra óptica sobre otros medios de transmisión.

El avance y desarrollo de este medio ha hecho que evolucione mejorando así algunas de sus características.

- Cobertura más resistente. La cubierta contiene un 25% más material que las cubiertas convencionales.
- Uso interior y exterior de la fibra gracias a su resistencia al agua y emisiones ultravioleta y su cubierta resistente.
- Mayor resistencia a la humedad por el recubrimiento en el interior de la fibra de múltiples capas de protección.
- Empaquetado de alta densidad. Con el máximo número de fibras en el menor diámetro posible se consigue una más rápida y fácil instalación donde el cable se puede enfrentar a ángulos agudos y espacios estrechos.

1.5.1.2 Radio Frecuencia

El término radiofrecuencia, también denominado *RF*, se aplica a la porción menos energética del espectro electromagnético, situada entre unos 3 Hz y unos 300 GHz. El Hertz (Hz) es la unidad de medida de la frecuencia de las ondas radioeléctricas, y corresponde a un ciclo por segundo. Las ondas electromagnéticas de esta región del espectro se pueden transmitir aplicando la corriente alterna originada en un generador a una antena.

Aunque se emplea la palabra *radio*, las transmisiones de televisión, radio, radar y telefonía móvil están incluidos en esta clase de emisiones de radiofrecuencia.

Las bandas de frecuencia son intervalos de frecuencias del espectro electromagnético asignados a diferentes usos dentro de las radiocomunicaciones.

Clasificación de las ondas en telecomunicaciones

SIGLAS	RANGO	NOMBRE	USO / EMPLEO
ULF	300 Hz a 3 kHz	Ultra baja frecuencia	Militar, comunicación en minas
VLF	3 kHz a 30 kHz	Muy baja frecuencia	Radio gran alcance
LF	30 kHz a 300 kHz	Baja frecuencia	Radio, navegación
MF	300 kHz a 3 MHz	Frecuencia media	Radio de onda media
HF	3 MHz a 30 MHz	Alta frecuencia	Radio de onda corta
VHF	30 MHz a 300 MHz	Muy alta frecuencia	TV, radio
UHF	300 MHz a 3 GHz	Ultra alta frecuencia	TV, radar, telefonía móvil
SHF	3 GHz a 30 GHz	Súper alta frecuencia	Radar
EHF	30 GHz a 300 GHz	Extra alta frecuencia	Radar

El espacio asignado a las diferentes bandas abarca el espectro de radiofrecuencia y parte del de microondas y está dividido en sectores. En telecomunicaciones se clasifican las ondas mediante un convenio internacional de frecuencias en función del empleo al que están destinadas:

1.5.2 Tecnologías de transmisión empleadas

1.5.2.1 ADSL

ADSL son las siglas de *Asymmetric Digital Subscriber Line* ("Línea de Suscripción Digital Asimétrica"). ADSL es un tipo de línea DSL. Consiste en una transmisión de datos digitales apoyada en el par simétrico de cobre que lleva la línea telefónica convencional o línea de abonado, siempre y cuando la longitud de línea no supere los 5,5 km medidos desde la Central Telefónica, o no haya otros servicios por el mismo cable que puedan interferir.

Frecuencias usadas en ADSL. El área verde es el área usada por la voz en telefonía normal, la roja es la subida de datos y la azul es para la descarga de datos.

Es una tecnología de acceso a Internet de banda ancha, lo que implica una velocidad superior a una conexión tradicional por módem en la transferencia de datos. Esto se consigue mediante una modulación de las señales de datos en una banda de frecuencias más alta que la utilizada en las conversaciones telefónicas convencionales (300-3800 Hz), función que realiza el router ADSL. Para evitar distorsiones en las señales transmitidas, es necesaria la instalación de un filtro que se encarga de separar la señal telefónica convencional de las señales moduladas de la conexión mediante ADSL.

Esta tecnología se denomina *asimétrica* debido a que la capacidad de descarga (desde la red hasta el usuario) y de subida de datos (en sentido inverso) no coinciden. Normalmente, la capacidad de bajada es mayor que la de subida.

1.5.2.2 MPLS

MPLS (*Multiprotocol Label Switching*) es un mecanismo de transporte de datos que opera entre la capa de enlace de datos y la capa de red del modelo OSI.

Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes. Puede ser utilizado para transportar diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP. Es una nueva tecnología de conmutación creada para proporcionar circuitos virtuales en las redes IP, sobre las que introduce una serie de mejoras:

- Redes privadas virtuales.
- Ingeniería de tráfico.
- Mecanismos de protección frente a fallos.

La tecnología MPLS ofrece un servicio orientado a conexión:

- Mantiene un estado de la comunicación entre dos nodos.
- Mantiene circuitos virtuales

En MPLS el camino que se sigue está prefijado desde el origen, se pueden utilizar etiquetas para identificar cada comunicación y en cada salto se puede cambiar de etiqueta, los paquetes destinados a diferentes direcciones IP pueden usar el mismo camino y las etiquetas con el mismo destino y tratamiento pueden ser agrupadas en una misma etiqueta.

1.5.2.3 Radioenlace

La tecnología de comunicación a través del radioenlace hace referencia a la interconexión entre terminales de telecomunicaciones efectuados por ondas electromagnéticas.

Los sistemas de comunicaciones radioenlaces entre puntos fijos proporcionan una capacidad de información, con características de calidad y disponibilidad determinadas. Típicamente estos enlaces se explotan entre los 800 MHz y 42 GHz

Los radioenlaces, establecen una comunicación del tipo dúplex, de donde se deben transmitir dos portadoras moduladas: una para la transmisión y otra para la recepción. Al par de frecuencias asignadas para la transmisión y recepción de las señales, se lo denomina radio canal.

Un radio enlace esta constituido por estaciones terminales y repetidoras intermedias, con equipos transceptores, antenas y elementos de supervisión y reserva.

Además de las estaciones repetidoras, existen las estaciones nodales donde se demodula la señal y de la baja a banda base y en ocasiones se extraen o se insertan canales.

1.5.2.4 VPN

Una VPN (V*irtual Private Network*), es una tecnología de red que permite una extensión de la red local sobre una red pública por ejemplo Internet.

Para hacerlo posible de manera segura es necesario proporcionar los medios para garantizar la autentificación, integridad y confidencialidad de toda la comunicación.

La autentificación y autorización en una VPN se realizan para verificar la identidad de los usuarios y restringir su acceso a aquellos usuarios que no estén autorizados.

La integridad de los datos enviados hace referencia al hecho de que los datos transmitidos no hayan sido alterados o modificados. Esto se consigue a través de complejos algoritmos, por ejemplo el SHA (Secure Hash Algoritm) o el MD2/MD5 (Message Digest)
Por último la confidencialidad de los datos se consigue utilizando algoritmos de cifrado, por ejemplo *Data Encryption Standard* (DES), Triple DES (3DES) o *Advanced Encryption Standard* (AES).

2. ESTADO INICIAL

Durante este capítulo se analizará en qué estado se encuentra la empresa en el momento que se decide realizar el cambio de infraestructura.

Se buscarán los puntos débiles que existen en la infraestructura tanto a nivel de WAN como a nivel local en las LAN de los almacenes.

2.1 Análisis inicial

En este apartado analizamos el estado del sistema de comunicaciones de la empresa en su fase inicial (2007).

El estudio que muestro a continuación refleja las carencias y los puntos débiles que tenemos en el sistema de comunicaciones para posteriormente buscar las soluciones y mejoras más apropiadas acorde con los recursos de la empresa.

Inicialmente cada sede de FDF cuenta con un servidor de recepción de pedidos que recibe estos a través de módems de 56kbps. De tal manera que cada socio realiza el pedido a su almacén a través de los teléfonos asociados a los módems y el almacén se encarga de realizar el pedido y servirlo.

En el caso de que algún almacén no disponga del artículo que el socio solicita, transmite dicha información a través del sistema de comunicaciones de la empresa a otro almacén que pueda realizar el pedido.

Aunque este es el estado básico inicial el análisis que se realiza a continuación se trata realmente de un periodo intermedio en el que se comenzaron a recibir pedidos por ADSL a través de dos servidores de recepción que se encontraban en la sede central de Barcelona que a su vez coexistía con el sistema de recepción de pedidos a través de módems.

2.1.1 Red WAN

A continuación se muestra un estudio del estado inicial del tráfico de los enlaces WAN que existían en la empresa.

Este estudio nos permitió optimizar el servicio que se presta a los usuarios, sacar conclusiones sobre la dimensión de los enlaces y validar la calidad de servicio (*QoS*) que prestaba el operador de comunicaciones que soporta la red de la empresa. En este caso el operador se trataba de Telefónica.

El análisis se realizó mediante el sistema de monitorización de comunicaciones *PacketShaper 3500 (*véase **Anexo 6.2***)* el cual se instaló entre los routers de comunicaciones WAN y la red interna.

En la **Fig. 2.3** se muestra el sistema de comunicaciones de la empresa al inicio del análisis.

La sede de Barcelona contaba con una conexión a la MPLS de 100Mbps donde se conectaban el resto de sedes (Telefónica garantizaba el 20% de los recursos contratados en fibra óptica). Terrassa y Hospitalet al producir más tráfico que el resto tenían una fibra óptica contratada de 20Mbps. Estas sedes con fibra óptica tienen un ADSL de back-up en caso de quedarse por alguna causa sin la línea principal.

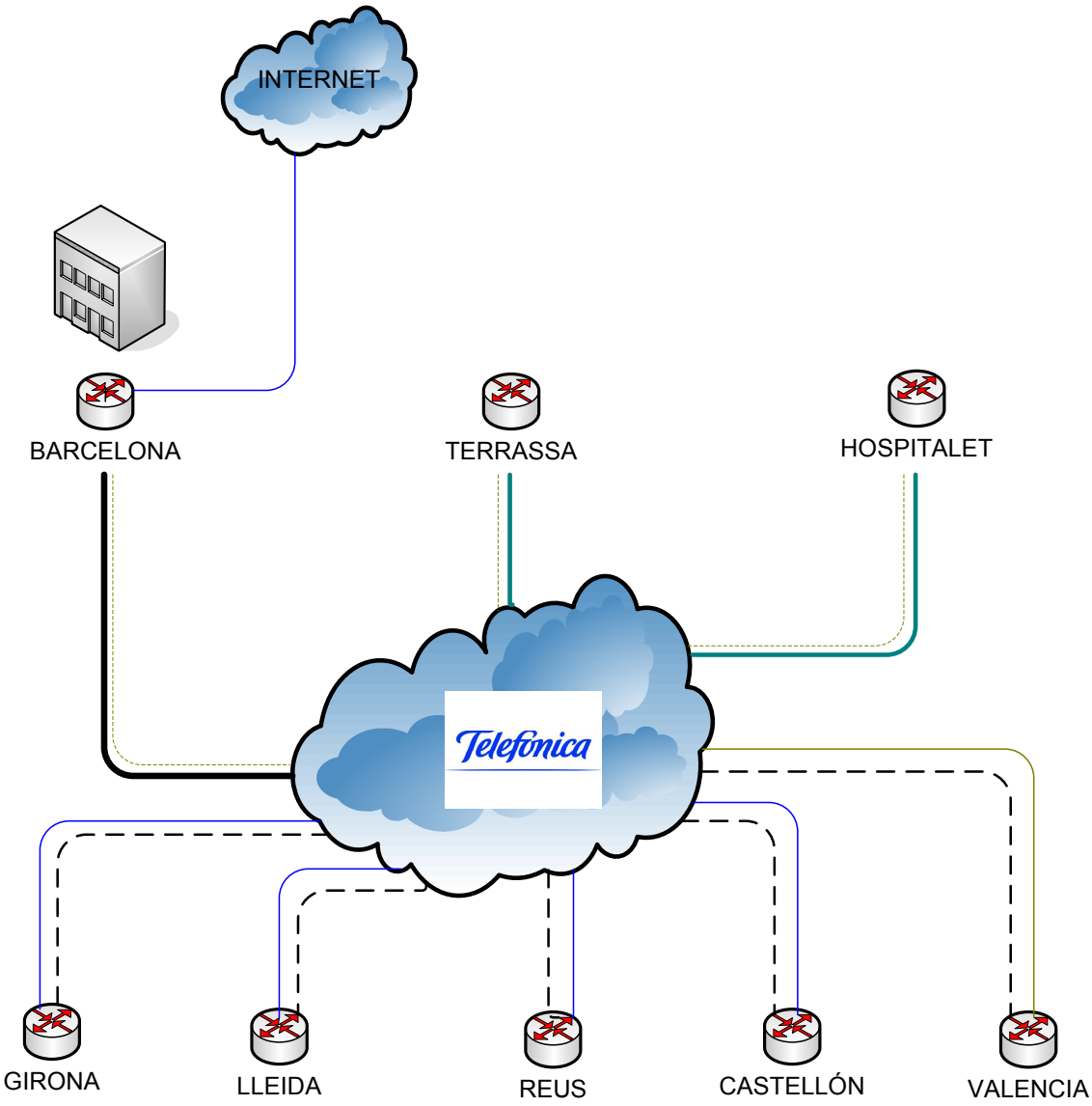
El resto de sedes tenían contratadas un ADSL de 2Mbps de bajada y 256kbps de subida excepto la sede de Valencia que tenia contratado un ADSL de 4Mbps de bajada y 500kbps de subida (Telefónica garantizaba el 10% de los recursos contratados en ADSL).

Todas las sedes contaban con una línea de RDSI (128kbps) que hacía de back-up en caso de perdida de conexión en la línea principal.

Aquí podemos encontrarnos con el problema, ya que en el caso de que por causas externas se quedase incomunicada una sede por el corte de la línea (por ejemplo cualquier tipo de construcción u obra) esta sede no podría recibir pedidos ya que tanto la línea de ADSL como la RDSI se transmiten a través del mismo par de cobre.

A parte podemos observar que en la delegación central de Barcelona, donde se encuentran dos servidores de recepción de pedidos posee una salida estándar de Internet 2Mbps (bajada) 256kbps (subida), donde se recepcionaban los pedidos de los socios.

Como hemos comentado anteriormente, todas las sedes contaban con módems de 56kbps donde los socios podían hacer pedidos a través de ellos (los módems mencionados no aparecen en la figura que se muestra a continuación).



Leyenda	
	Fibra óptica 100Mbps
	Fibra óptica 20Mbps
	ADSL 4Mbps
	ADSL 2Mbps
	RDSI Back-up
	ADSL 2Mbps Back-up
	Router sede

Fig. 2.3 Mapa de comunicaciones de FDF en su fase inicial

2.1.1.1 Problemas WAN

En este apartado se extraen los datos más relevantes que se han obtenido en el estudio de la red WAN de la empresa y que permiten aportar un mayor entendimiento del estado de la red.

Todas las gráficas que se muestran a continuación están hechas durante una semana de periodo. En el caso de que no sea así, se especificará dentro de la explicación de la gráfica.

El siguiente gráfico (**Fig. 2.4**) se muestra el tráfico *entrante* y *saliente* en la delegación de Barcelona durante una semana.

El *Packetshaper* 3500 *(*véase **Anexo 6.2***)*, se coloca en la delegación de Barcelona, para controlar la comunicación de esta sede central con el resto de sucursales. El dispositivo, se coloca como elemento intermedio entre la LAN de la sede y el router de acceso a la MPLS.

Podemos observar como se van sucediendo drásticas subidas y bajadas del tráfico tanto en la entrada como en la salida. La explicación que damos a estas oscilaciones de tráfico se debe a la demanda de pedidos que sufre la empresa en momentos puntuales a lo largo del día y como consecuencia provoca procesos como la validación del pedido o la inserción del pedido en la base de datos, que a su vez generan más tráfico en la MPLS.

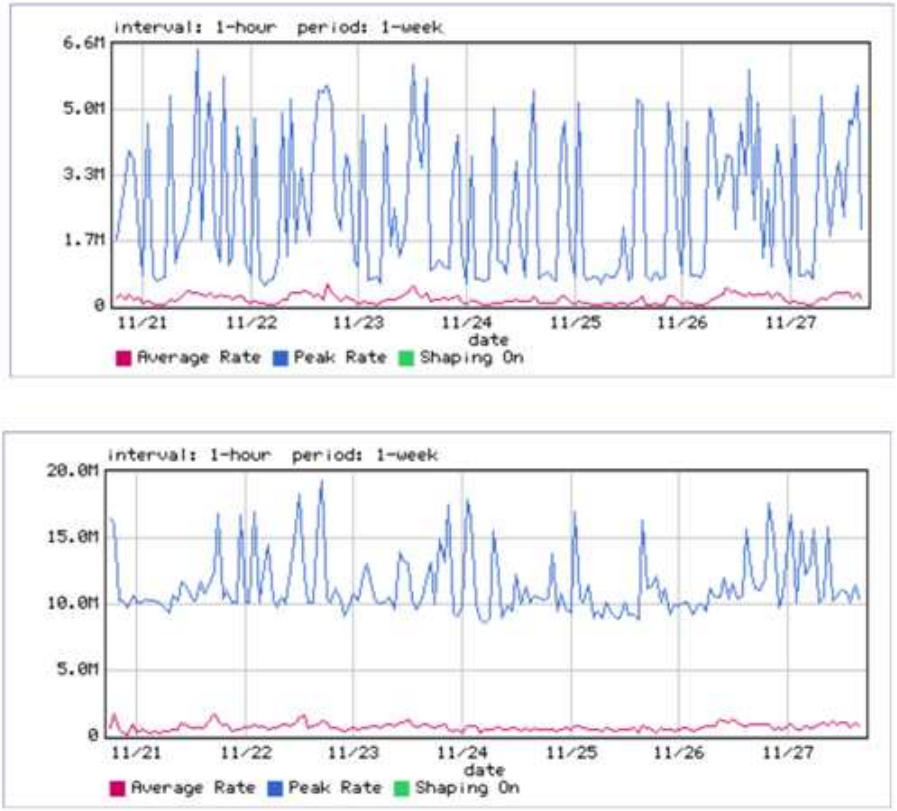


Fig. 2.4 * Tráfico entrante y saliente de la delegación de Barcelona (Enlace F.O. Barcelona – MPLS TESA)

(*) Debemos de tener en cuenta que el ancho de banda entrante es el tráfico saliente de la plataforma y viceversa.

La empresa tiene unas horas críticas en las cuales es de vital importancia que el sistema funcione correctamente, en base a estos tramos horarios se realiza el dimensionado del sistema de comunicaciones. El mayor volumen de tráfico es recibido en los siguientes intervalos horarios (en especial en el tramo del mediodía):

- 13:30 h - 14:30 h
- 20:30 h - 21:30 h

Estas horas corresponden al cierre de mediodía y cierre vespertino de la mayoría de las OF que aprovechan el cierre de sus comercios para realizar el pedido a su distribuidor de medicamentos, y digo mayoría ya que como todos sabemos existen las OF 12 o 24 horas.

Como se puede observar en la gráfica del tráfico *entrante*, los picos de tráfico nunca bajan de cierto nivel como consecuencia del tráfico broadcast que se encuentra en la red. Este tráfico continuo es aún más evidente en la segunda gráfica, donde el valor del tráfico *saliente* nunca baja de 10 Mbps

Telefónica, nuestro proveedor de servicios MPLS, garantizaba el 20% del ancho de banda (BW, *Bandwith*) de sus enlaces de fibra en aquel momento por lo que:

$$BW\ garantizado = BW\ contratado \cdot 0{,}2$$

En este caso el enlace monitorizado se trata de un enlace de fibra óptica de 100Mbps del cual se garantiza 20Mbps (tanto en la subida de tráfico como en la bajada).

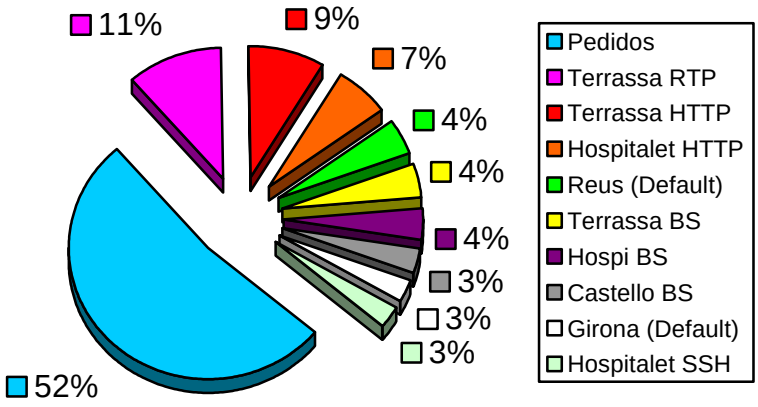
En algunos puntos de la gráfica (**Fig. 2.4**), el tráfico llega a acercarse a este límite de 20Mbps (durante las horas críticas). Se tendrá que tener en cuenta este dato a la hora de contratar el ancho de banda que garantice el ISP actual o el nuevo ISP que se contrate para darnos servicio.

Otro punto a analizar es el tipo de tráfico que pasa por nuestra red para evaluar si se hace un buen uso de ella.

Para ello se realizó un análisis en el cual mostraba las diferentes clases de tráfico y el porcentaje de uso que daban sobre la red.

A continuación se muestran las principales clases de tráfico que están consumiendo tráfico para las conexiones entrantes y salientes (**Fig. 2.5**) del tráfico mostrado en la figura anterior (**Fig. 2.4**). La mayoría del tráfico monitorizado se puede valorar como tráfico importante dentro del funcionamiento de la empresa. El único tráfico a destacar que carece de importantica es el tráfico de Voz sobre IP (VoIP) de la delegación de Terrassa (protocolo RTP), el consumo de enlace que realiza este tipo de tráfico hace que la utilización del enlace sea inferior (alrededor del 10%).

Clases de tráfico entrante



Clases de tráfico saliente

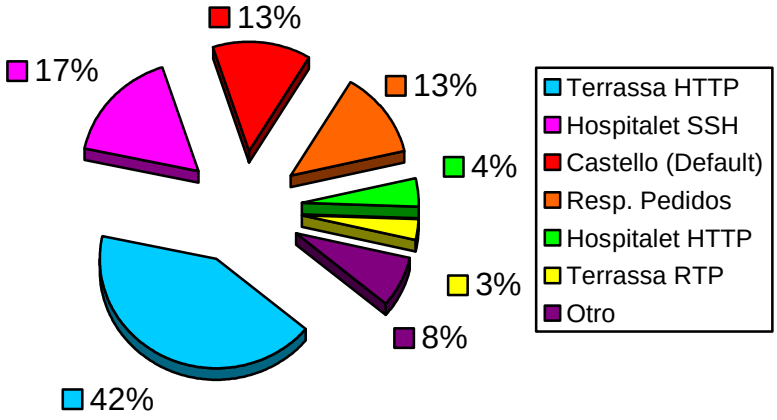


Fig. 2.5 Clases de tráfico que se observa en la entrada y salida de la WAN (Enlace F.O. Barcelona – MPLS TESA)

A continuación se muestra una breve descripción de cada clase de tráfico:

- El volumen de tráfico de *Pedidos*, corresponde al tráfico que generan los pedidos realizados por los socios contra nuestros servidores de recepción, más de la mitad del tráfico entrante. En la salida la *Respuesta Pedidos* tiene un valor inferior, esto se debe a que la respuesta que damos al socio precisa menos volumen de información.

- El tráfico *HTTP* corresponde al tráfico que se genera en las diferentes sedes por el uso de conexiones a Internet, el uso de ciertas aplicaciones hacen que Internet sea una herramienta usada por la empresa.

- El tráfico *BS* hace referencia al tráfico generado por el sistema informático que utilizaba la empresa en ese momento, *BS2000*.

- El tráfico *SSH* hace referencia al tráfico que generan las conexiones que realizan las sedes contra la sede central para realizar una serie de procedimientos.

- Las sedes que pone *Default* hacen referencia a todos estos tipos de tráfico mencionados con anterioridad que se han juntado en una sola muestra debido al poco volumen de tráfico que generan, de esta forma podemos ver el peso que tienen todas las sedes en el tráfico total.

Tráfico en delegaciones

La siguiente gráfica es una muestra de los picos de tráfico de la delegación de Valencia (**Fig. 2.6**). Es importante observar que el enlace de subida del ADSL se satura a los 250 kbps, este hecho muestra la incapacidad de la línea para soportar los momentos de máxima carga. Esta misma conclusión se puede extraer de las delegaciones de Castellón, Reus y Lleida.

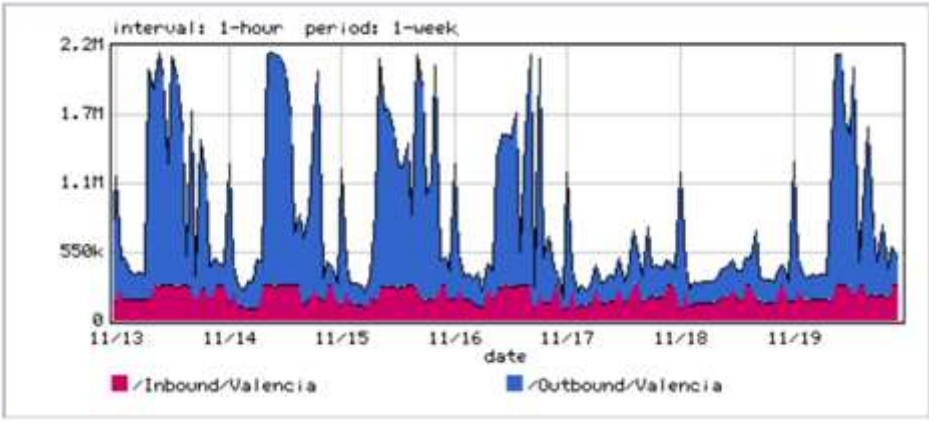


Fig. 2.6 Tráfico entrante y saliente de la delegación de Valencia (enlace delegación Valencia – MPLS TESA)

2.1.1.2 Conclusiones WAN

Una vez encontradas las carencias en la MPLS se pueden extraer las siguientes conclusiones:

De carácter general se puede observar los siguientes detalles:

- La capacidad de casi todos los enlaces (exceptuando Terrassa y Barcelona) es insuficiente para soportar el tráfico generado en horas de máxima carga sin ninguna priorización del tráfico, se producen saturaciones.

- Todas las delegaciones se concentran en el switch de entrada de la central de Barcelona. En caso de que hubiera algún problema en este equipo, las delegaciones quedarían aisladas.

- El tráfico de VoIP generado por la delegación de Terrassa (**Fig. 2.5**) deberá limitarse para que no produzca problemas de rendimiento de enlace, esto se puede solucionar utilizando una serie de mecanismos y técnicas que lo limiten.

- La necesidad de reducir el impacto del tráfico *broadcast* reduce la capacidad útil de la red.

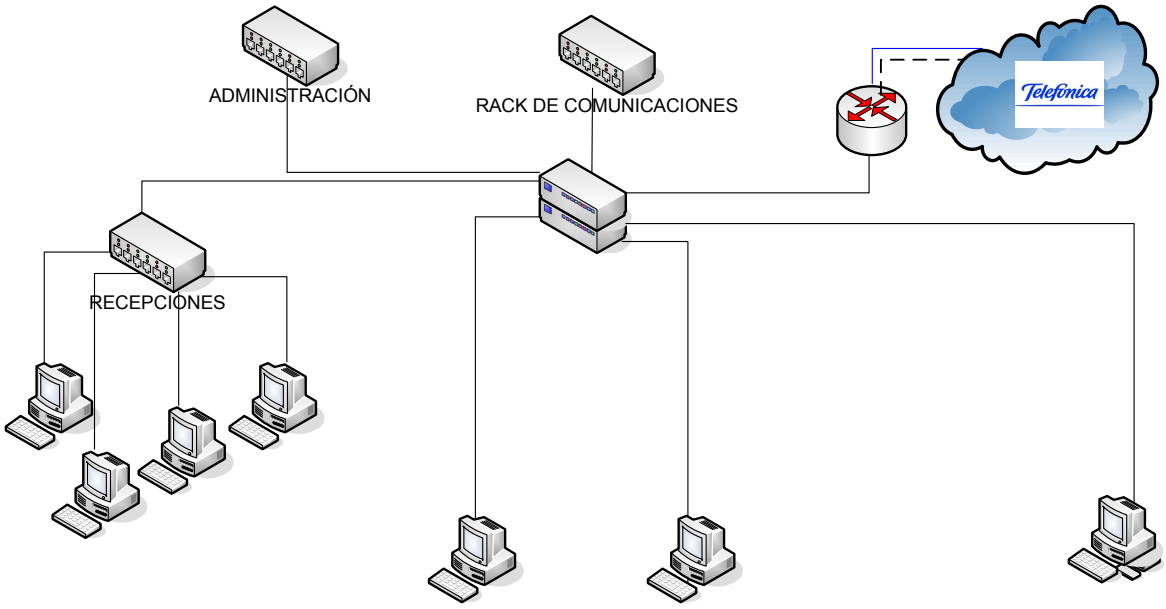
- La criticidad de poder quedarse una sede incomunicada a causa de la perdida del único medio de comunicación que se posee es extrema ya que el mismo sistema no desvía el pedido del socio hacía otro almacén.

2.1.2 Redes LAN sedes

Como ya se ha comentado con anterioridad, esta empresa esta compuesta por varias sedes distribuidas por el territorio catalán y parte de la comunidad valenciana. Todas estas sedes (almacenes) han sido analizadas inicialmente para ver las carencias de sus redes LAN.

Para realizar las pruebas de tráfico se han empleado herramientas específicas de análisis de protocolos de red, como es el *Sniffer Pro (*véase **Anexo 6.2***)* para hacer las capturas de tráfico.

Ya que todos los almacenes mantienen la misma topología de red y los mismos elementos de interconexión, mostraremos el mapa de comunicaciones de un almacén de ejemplo, en este caso el almacén de Valencia (**Fig. 2.7**):



Leyenda	
	Cableado LAN
	Switch almacén
	Hub almacén
	PC Operario
	ADSL 2Mbps / 256kbps
	RDSI
	Router almacén

Fig. 2.7 Mapa de comunicaciones de un almacén estándar de FDF

2.1.2.1 Problemas LAN

Una vez comentados los puntos a tener en cuenta en diseño de la WAN se hace un estudio del estado de la LAN de las diferentes sedes para poder comprobar su rendimiento y analizar problemas que tengan.

A continuación se enumeran los diferentes problemas que se han encontrado en el cómputo global de todas las delegaciones:

- Problemas de Antivirus
- Problemas de tráfico broadcast
- Enlaces de más de 100m y de baja calidad
- Errores de puertos mal configurados
- Elementos de interconexión no gestionables
- Cableado UTP en mal estado

A continuación se detallan cada uno de estos puntos:

Problemas de Antivirus

En la **Fig. 2.8** se muestra un análisis de las conexiones que se producen en la LAN de la sede de Castellón.

En este proceso de monitorización nos damos cuenta de un hecho aislado, poco habitual y debido a las consecuencias que puede repercutir en el tráfico de la red he creído importante mencionar. La monitorización de este evento fue de tan solo tres horas, pero la rareza de los datos que extraje fue razón suficiente para que fuera analizado.

La mayor parte del tráfico generado en la LAN (el 90% del tráfico), se produce de la comunicación que mantienen estas dos direcciones IP: 172.16.201.71 y 172.16.70.10, mientras que el resto de comunicaciones son internas y tienen un tráfico menor.

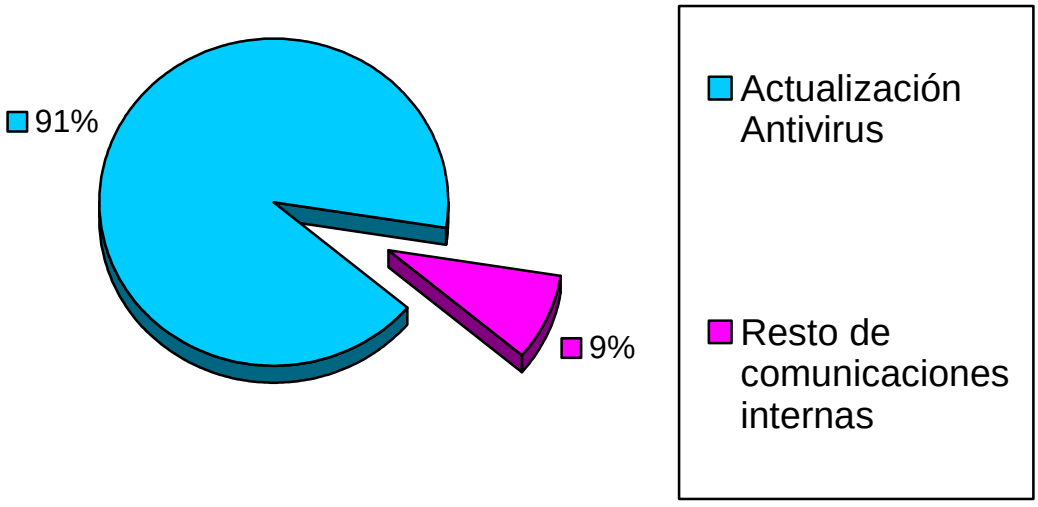


Fig. 2.8 Análisis de la LAN en la delegación de Castellón

La primera de las direcciones IP corresponde a un servidor de antivirus situado en la sede de Barcelona y la segunda corresponde a un PC de la delegación de Castellón. Siguiendo la incidencia se detecta que el equipo del usuario estaba actualizando su antivirus contra el servidor y estaba generando esa cantidad tan importante de tráfico.

El volumen de datos de esta actualización representa el aumento de tráfico en el enlace de 10 kbps a 200 kbps.

Problema de tráfico broadcast

En la gráfica siguiente (**Fig. 2.9**) se puede observar como en la delegación de Barcelona un 10% del tráfico pertenece a tráfico broadcast (172.16.233.255). En este caso se realiza una monitorización semanal del tráfico interno de la LAN de Barcelona. La mayor parte de este tráfico esta generado por *elementos de interconexión no gestionables*.

Cuando hablamos de *elementos de interconexión no gestionables* nos estamos refiriendo a aquellos dispositivos que conectan partes de una red y no tienen la capacidad de poder ser administrados por un usuario. Un ejemplo de este tipo de elementos son los hub, dispositivos que operan a nivel físico que no requieren ningún tipo de configuración debido a su sencillez. Un hub tiene como misión repetir toda la información que recibe a todo el que esté conectado a él y esto es lo que provoca el tráfico broadcast.

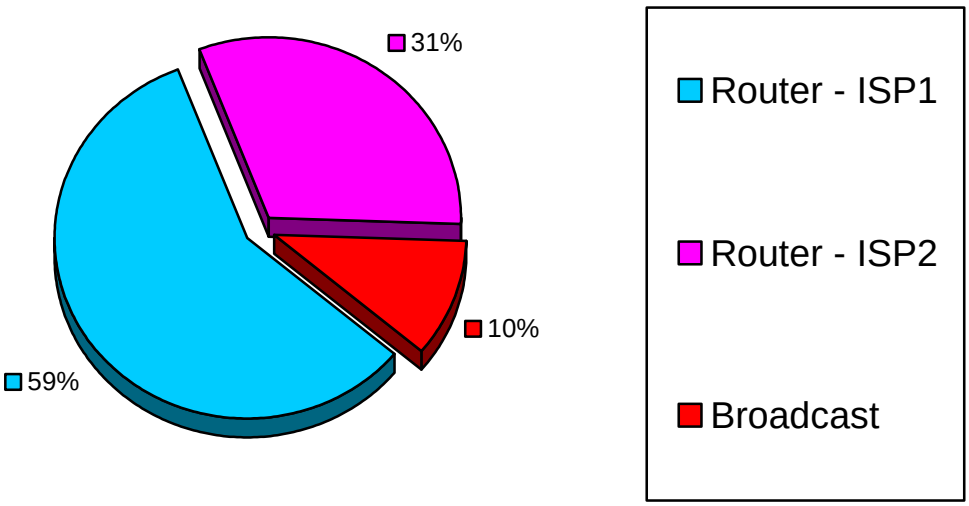


Fig. 2.9 Conexiones generadas en la delegación de Barcelona

Las dos primeras conexiones que muestra la leyenda de la **Fig. 2.8** hacen referencia a conexiones que establece el switch *Core (*véase **Anexo 6.2***)* de Barcelona contra las dos direcciones IP públicas que nos proporcionaba nuestro proveedor de Internet, lo que representa un 87% del tráfico escaneado. El resto se trata de conexiones internas entre usuarios y el 10% del tráfico broadcast mencionado anteriormente.

Enlaces de más de 100 metros y de baja calidad

Los tramos de cableado superiores a 100 metros añaden lentitud a la transmisión y problemas en la red. Este tipo de enlaces los podemos encontrar en todas las sedes de las diferentes delegaciones. En la **Fig. 2.10** se muestra un análisis en la LAN de la delegación de Lleida. La figura muestra un análisis del cual filtramos los errores para que sean analizarlos.

Duration	Se...	Description	Object
1m 56s 339ms	Minor	Window Size Exceeded	TCP: [172.16.70.36] - [172.16.201.117] Port 35122 - 80
1m 51s 758ms	Minor	Window Size Exceeded	TCP: [172.16.70.41] - [172.16.201.111] Port 60235 - 80
1m 49s 58ms	Minor	Zero Window Too Long	TCP: [172.16.70.29] - [172.16.201.117] Port 9100 - 4...
1m 19s 181ms	Minor	Window Frozen	TCP: [172.16.70.36] - [172.16.201.117] Port 45597 - 80
1m 16s 299ms	Minor	Window Frozen	TCP: [172.16.70.41] - [172.16.201.111] Port 60235 - 80
1m 16s 228ms	Minor	Window Frozen	TCP: [172.16.70.41] - [172.16.201.111] Port 60236 - 80
<1ms	Minor	Ack Too Long	TCP: [172.16.70.36] - [172.16.201.117] Port 45598 - 80
<1ms	Minor	Ack Too Long	TCP: [172.16.70.36] - [172.16.201.117] Port 45598 - 80
1m 9s 102ms	Minor	Window Frozen	TCP: [172.16.70.36] - [172.16.201.117] Port 45598 - 80
<1ms	Minor	Ack Too Long	TCP: [172.16.70.36] - [172.16.201.117] Port 45599 - 80
<1ms	Minor	Ack Too Long	TCP: [172.16.70.36] - [172.16.201.117] Port 45599 - 80

Fig. 2.10 Análisis de paquetes en la LAN de Lleida

Los errores que muestra el análisis son: *ACK too long, Idle too long, Window Frozen* y *Window Size Exceeded*. Estos mensajes se deben en su mayoría a la lentitud de los enlaces y la degradación de estos durante la transmisión, lo cual provoca la retransmisión de nuevos paquetes y de esta manera baja la eficiencia de estos enlaces que están ubicados en las diferentes sedes.

- *ACK too long*. Hace referencia al tiempo de respuesta de los paquetes que se transmiten. Si en ese tiempo no se recibe el ACK, se retransmite el paquete, lo que provoca retransmisiones innecesarias en la red.

- *Idle too long.* Este error nos informa de que se ha superado el tiempo máximo de inactividad en el enlace.

- *Window Frozen.* El tamaño de ventana es un parámetro que viene configurado en el protocolo TCP para conseguir más eficiencia en los enlaces. Si tenemos retardos se activa el mecanismo de ventana congelada para evitar errores y hace que el tamaño de la ventana no siga creciendo.

- *Window Size Exceeded.* Este error tiene que ver con el anterior, habla también del valor del tamaño de la ventana de transmisión de TCP, y se queja de que su valor máximo ha sido sobrepasado.

Puertos mal configurados

Como en toda red de área local nos encontramos con elementos de interconexión (Hubs, Switches, concentradores, Routers,…) que administran y conectan a los usuarios que usan la red. Estos elementos que tiene la función de conectar, lo hacen a través de los puertos que tienen. Ahora hablaré de los puertos de los que constan los elementos de interconexión y que por algún motivo de configuración hacen que no funcionen adecuadamente. Esto hace que se provoquen una serie de fallos y como consecuencia afecta a la eficiencia de la red.

A la hora de revisar todos los elementos de la red nos encontramos con graves problemas de configuración en casi todas las sedes. A continuación mostramos varios ejemplos de esta clase de problemas.

Tomamos un ejemplo de un servidor situado en la sede de Valencia, en la **Fig. 2.11** podemos ver un elevado número de tramas broadcast. La causa de esto son los elementos no gestionables que encontramos en la LAN.

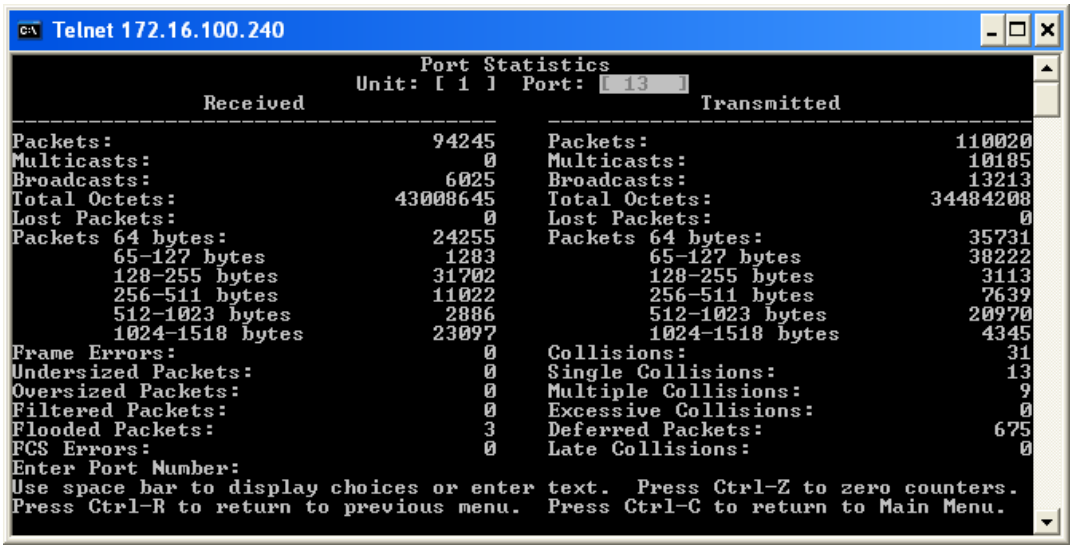


Fig. 2.11 Estadística de transmisiones y recepciones del puerto 13 del switch principal de la delegación de Valencia

Por ejemplo, en la **Fig. 2.12** se puede observar como los puertos 19 y 24 de la delegación de Reus tiene los puertos deshabilitados o el puerto 18 habilitado pero configurado a 10 Mbps y en modo *Half-Duplex.*

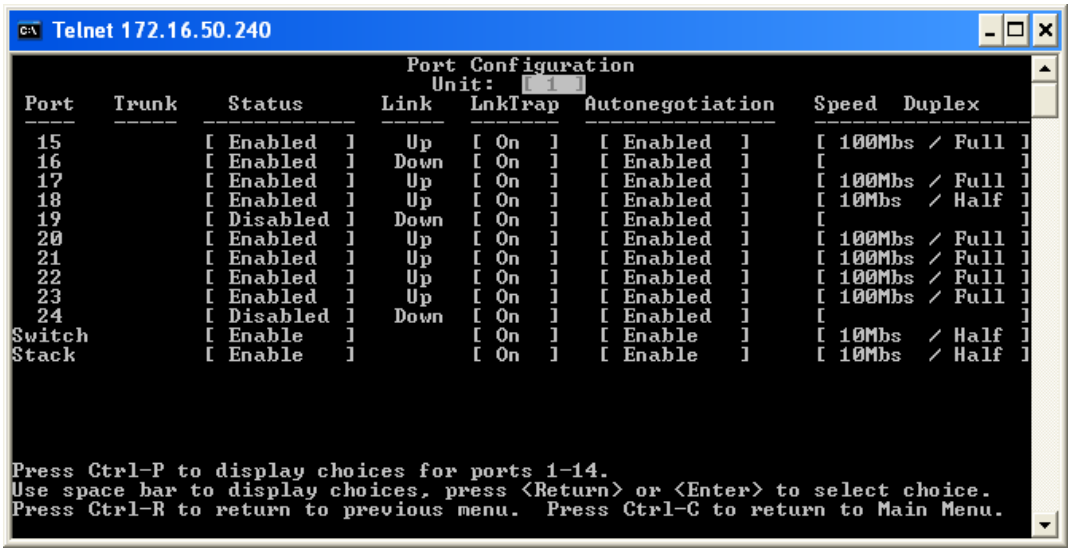


Fig. 2.12 Vista de la configuración de los puertos de un switch de Reus

En la **Fig. 2.13** encontramos errores en la delegación de Lleida provocados por la colocación del un *Hub* como elemento *Core (*véase **Anexo 6.2***)* de esta delegación. Esto provoca errores en puertos forzados por la instalación de elementos no gestionables.

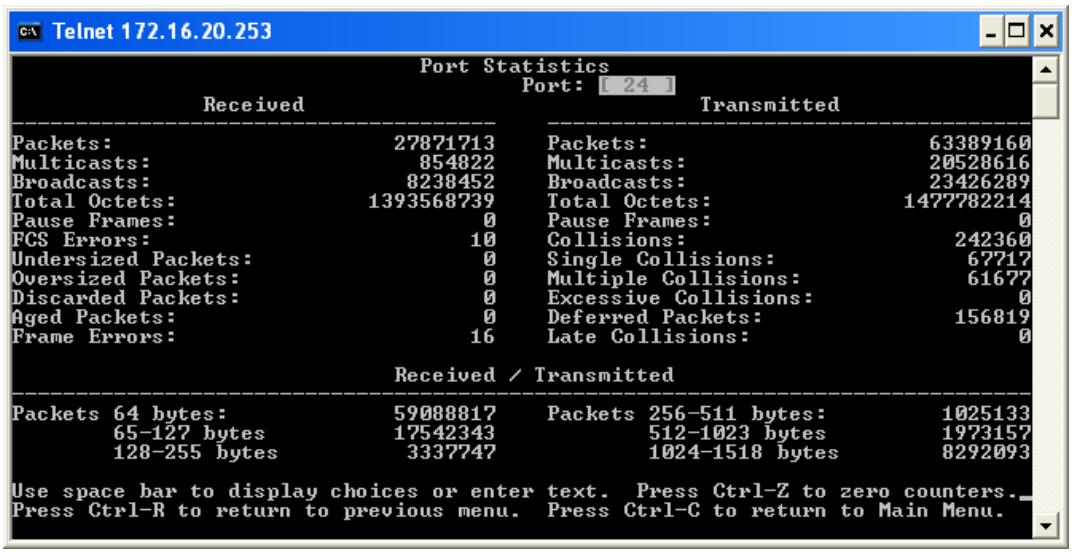


Fig. 2.13 Estadística de las transmisiones y recepciones del puerto 24 del switch principal de la delegación de Lleida

Elementos de interconexión no gestionables

Los elementos de interconexión no gestionables son aquellos elementos de la red que se encargan de conectar partes de una red y dichos elementos tienen un nivel de operación mínimo ya que no pueden ser controlados por ningún usuario.

Hubs (**Fig. 2.14**) y concentradores de capa 2 que únicamente sirven para conectar un número limitado de equipos son un ejemplo de esta clase de elementos. Este tipo de hardware provoca con su funcionamiento la perdida de eficiencia en la red, añadiendo tráfico broadcast a esta.

Fig. 2.14 Hub D-LINK de FDF en Reus

Cableado UTP en mal estado

Las instalaciones de estos almacenes son muy antiguas y están poco cuidadas. Por esta razón nos encontramos con el problema que exponemos a continuación. Existen tramos de cableado (UTP de categoría 5) sin apantallar y con conectores que no están correctamente montados.

A parte existe el problema de la diafonía *(*véase **Anexo 6.2***)* ya que encontramos cableado eléctrico cercano al de red como es el caso de la delegación de Terrassa.

2.1.2.2 Conclusiones LAN

Las conclusiones que se pueden extraer del análisis realizado en el global de las redes locales de FDF son:

- Abordar una reestructuración de la red tanto lógica como a nivel de topología para poder tener redundancia en los principales equipos y enlaces de la red de cada sede. En la actualidad la caída de uno de los switch de salida de una delegación puede producir una caída total del servicio de la sede.

- Estudiar la necesitad de coordinar las actualizaciones de antivirus en los equipos de los empleados para no saturar la red en momentos de máxima necesidad de recursos.

- Repasar el cableado de máxima longitud 100 metros, ya que a mayor longitud mayor retardo, este aumento de retardo puede provocar retransmisiones según el protocolo de comunicación que se use y degradación de la señal.

- Repasar la canalización del cableado para evitar interferencias con otro tipo de cableado.

- Evaluar la necesidad de sustituir los elementos de red, ya que; o no se tiene soporte técnico por parte del fabricante, o no muestran un funcionamiento correcto y están obsoletos en algunos casos.

- Resulta imprescindible analizar la configuración de los puertos de toda la electrónica con el fin de evitar problemas de colisiones y errores.

- Existe la necesidad de segmentar la red en diferentes VLAN (Minimizar los efectos del broadcast, aumentar la seguridad de los equipos de electrónica y acceso a recursos de la red).

- Colocar elementos de red gestionables en los puntos *Core (*véase **Anexo 6.2***)* de la red.

3. SOLUCIÓN ADOPTADA

FDF en la actualidad se encuentra inmersa en una profunda transformación a todos los niveles.

Las oficinas centrales de la Cooperativa se trasladaron en julio de 2009 al que es el nuevo almacén de FDF en Gavà. Este almacén que inició su actividad a mediados de 2010 se ha convertido en el corazón logístico de la empresa.

En este capítulo se exponen las decisiones que se han tomado para solventar los problemas encontrados en el análisis del estado inicial, las cuales han producido una mejora general en todo el sistema.

3.1 Mapa actual de la red

En el estudio del estado inicial del sistema se pudo observar como la capacidad del ancho de banda de algunos enlaces resultaba insuficiente en algunos casos o muy limitado en otros. Por esta razón el primer punto a explicar es el cambio de las capacidades de los enlaces en la red de FDF y ver el mapa actual en el que se encuentra.

Para comenzar, comentar que en la actualidad FDF ha realizado un cambio en el proveedor de servicios, COLT Telecom pasa a encargarse de esto. COLT pretende ofrecer un nivel alto de eficiencia en sus enlaces y esto lo consigue realizando un sistema donde exista alta disponibilidad. En el apartado **3.2** explicamos el proceso en el cambio de proveedor de servicios.

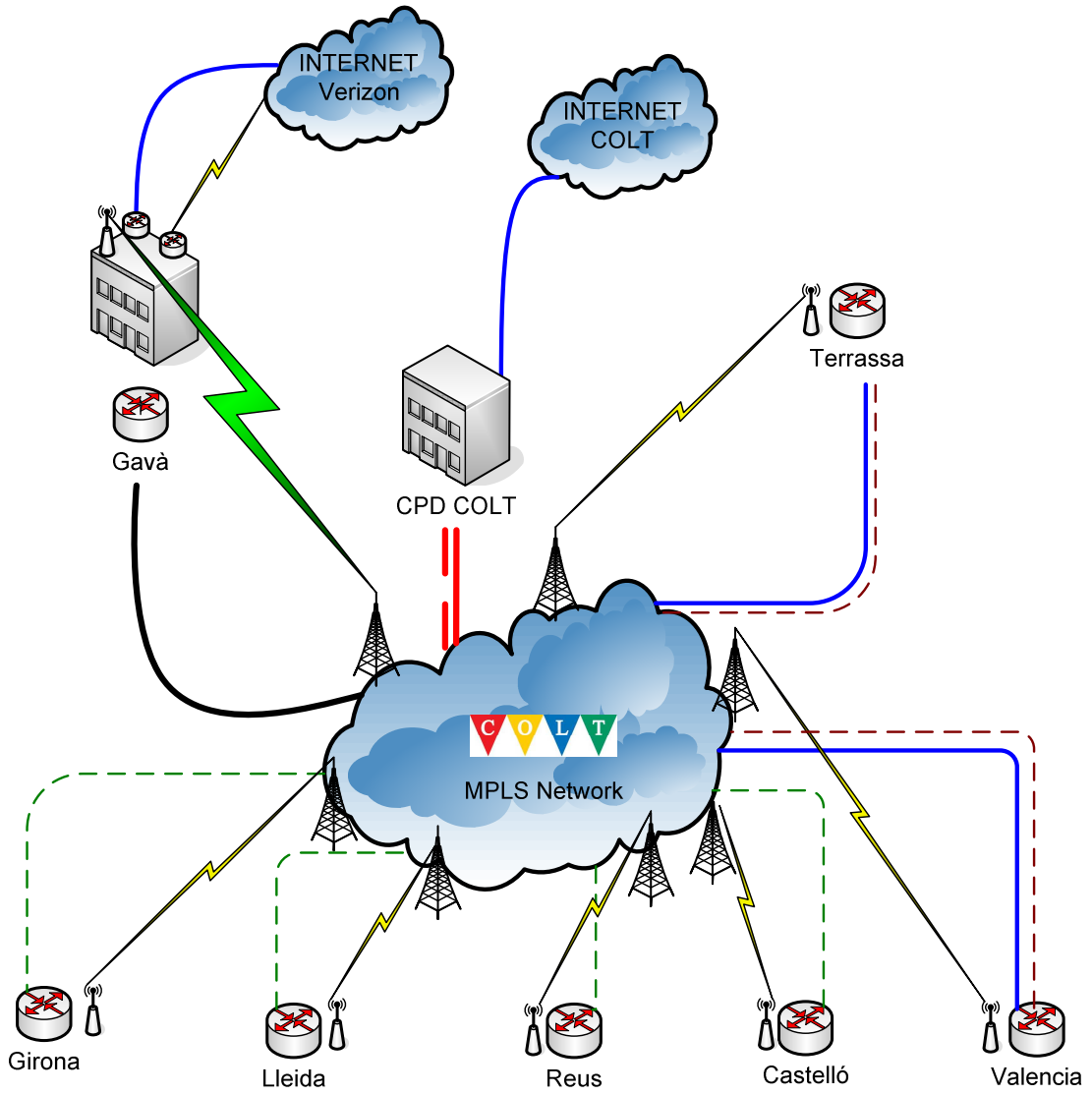
La solución propuesta e implementada se basa en dotar a cada sede dos vías de comunicación; en el caso de las sedes de Valencia y Terrassa el enlace principal está compuesto por fibra óptica de 4Mbps y un radioenlace de 4Mpbps que suman sus anchos de banda (8Mbps) para crear éste y una línea de back-up que corresponde a una línea SHDSL de 2Mbps.

En el resto de sedes mantienen el mismo patrón suprimiendo la fibra óptica, de tal manera que mantienen como línea principal el radioenlace de 4Mbps y tienen como línea de back-up un ADSL de 4Mpbs.
Mientras en la sede central de Gavà se mantienen las dos vías de comunicación pero la capacidad de los enlaces es mucho mayor, tenemos en este caso la fibra óptica de 32 Mbps como línea principal y el enlace por radiofrecuencia con 20 Mbps como línea secundaria.

Las líneas ADSL y SHDSL tienen un 50% de ancho de banda, mientras que las fibras ópticas tienen el 100% de ancho de banda garantizado por el proveedor.

Por último comentar que la fibra óptica que proporciona COLT para Internet es de 4Mbps pero puede ser excedida hasta un máximo de 20Mbps y la entrada de Internet en las oficinas de Gavà se hace a través de *Verizon*, que nos proporciona 4Mbps. En la **Fig. 3.2** se realizará una explicación más detallada de esto.

La **Fig. 3.1** muestra un mapa del estado de la red actual



Leyenda	
	FO 32Mb
	FO 4Mb
	FO 12Mb
	ADSL 4Mbps Back-up
	SHDSL 2Mbps Back-up
	FO 12Mb Back-up
	RE 20Mb Back-up
	RE 4Mb
	Antena RE
	Router sede RE
	Router sede cable

Fig. 3.1 Mapa de red actual

En la **Fig. 3.2** se muestra el diseño para el acceso a Internet que hay configurado en Gavà desde el cual se reciben una parte del total de los pedidos. Esta salida de Internet se realiza a través de *Verizon**. Como se puede ver disponemos de una salida por fibra (compuesta por dos fibras de 2Mbps cada una) y otra por radio de 2Mbps, como siempre, buscando la alta disponibilidad.

(*) *Verizon* es el proveedor de servicios que tenemos contratado en Gavà para la salida a Internet

Para esta recepción de pedidos tenemos dos direcciones IP públicas proporcionadas por *Verizon*. Nuestro *Checkpoint (*véase **Anexo 6.2***)* reenvía a la IP virtual del balanceador de carga (véase apartado **3.5**) donde están configuradas las direcciones IP virtuales de los servidores de recepción de pedidos.

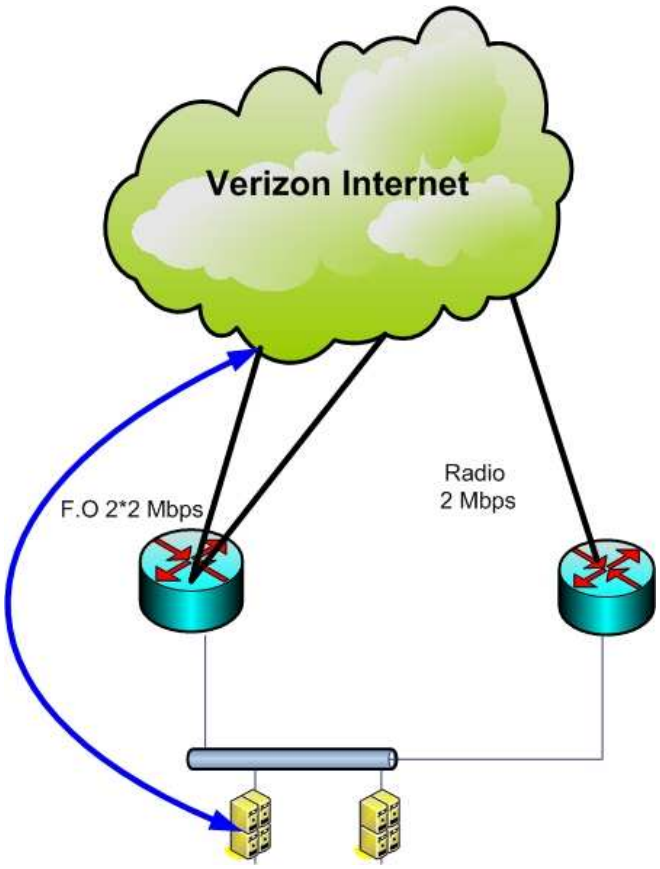


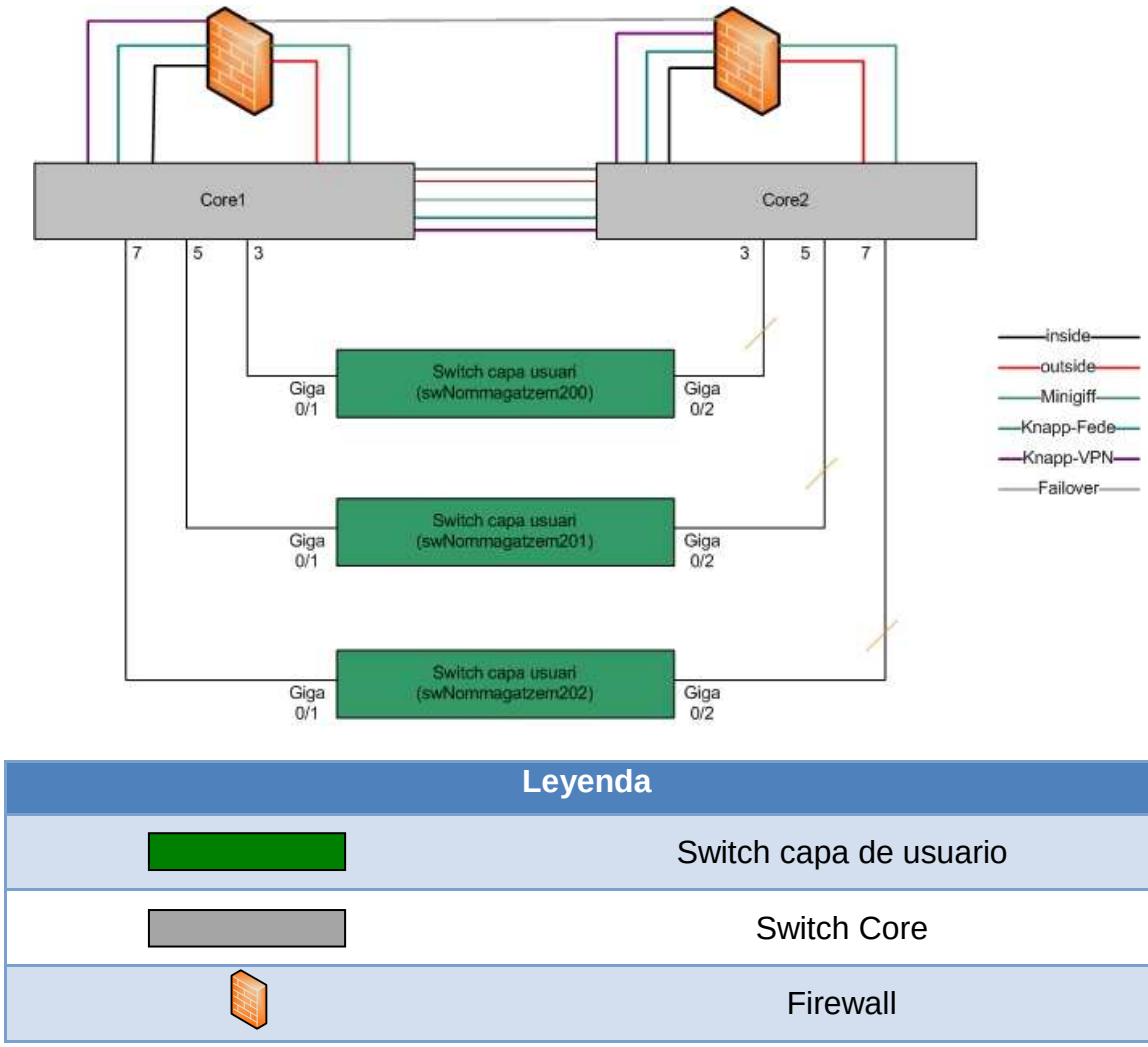
Fig. 3.2 Recepción pedidos Gavà

Hacemos también un pequeño análisis de la estructura que tienen los almacenes.

En cualquier caso, para cualquier modelo, el funcionamiento a nivel de *routing* para todos los almacenes siempre será el mismo. Nuestros equipos de capa 3 tendrán como puerta de enlace predeterminada (*default-gateway*) la dirección IP virtual que nos proporcione el protocolo HSRP en ese instante (*Hot Standby Router Protocol)*.

HSPR es un protocolo propiedad de CISCO que permite el despliegue de routers redundantes tolerantes a fallos en una red. Este protocolo evita la existencia de puntos de fallo únicos en la red mediante técnicas de redundancia y comprobación del estado de los routers. Este protocolo permitirá la comunicación entre nuestro hardware y el de Colt.

En la **Fig. 3.3** se muestra la estructura de red que tienen las sedes de FDF en la actualidad. Los almacenes tienen "n" switches de capa de usuario donde se conectan los ordenadores, impresoras, y demás elementos que requieran estar conectados a la red.



Leyenda	
	Switch capa de usuario
	Switch Core
	Firewall

Fig. 3.3 Mapa de comunicaciones general en una sede

Estos switches de capa de usuario están conectados a Core1 y a Core2 *(*véase **Anexo 6.2***)* que son switches de capa 3 que se encargan del *routing* de la red, el switch Core2 estará bloqueado a través del protocolo STP *(*véase **Anexo 6.2***)* que se encargará de que, en el caso de que el Core1 dejase de funcionar; active las comunicaciones con el switch Core2 para mantener las comunicaciones de la red. De esta forma nos aseguramos que siempre tenga la LAN y la WAN disponibles para nuestros usuarios.

Además se puede observar como las comunicaciones definidas entre el Core2 y los Switches de capa de usuario quedan deshabilitadas a causa de STP. Estás conexiones solo se habilitarán en el caso de que el enlace que está activo en el Core1 deje de estarlo por algún motivo (caída del equipo Core1, error en los puertos de conexión,…)

En caso de que uno de los switches de la capa de usuario dejase de funcionar, en todos los almacenes tenemos el switch con nombre swAlmacén200 como back-up de estos.

En los switches Core *(*véase **Anexo 6.2***)* tenemos conectados firewalls para dotar al almacén de seguridad (también se tiene alta disponibilidad en este aspecto).

Entre sí, los Core tienen varias conexiones que se repiten en cada almacén y que ahora comentaremos una a una:

- *Inside*. Esta conexión hace referencia al trafico entrante del Firewall al Core.
- *Outside*. Esta conexión hace referencia al trafico saliente del Core al Firewall.
- *Minigiff*. La siguiente conexión hace referencia al tráfico de pedidos de FDF correspondiente a cada sede, que asigna el sistema para que se realice el pedido al socio.
- *Knapp – FDF*. Es la conexión que comunica el sistema de pedidos con Knapp *(*véase **Anexo 6.2***)*
- *Knapp – VPN*. Esta conexión sirve para que el servicio técnico de Knapp (que se encuentra en Austria) se conecte al almacén en caso de avería.
- *Failover (*véase **Anexo 6.2***)*. Por último, esta conexión permite commutar de un Firewall a otro en caso de caída del principal.

Cabe comentar que todas la comunicaciones están definidas entre los dos Core para evitar perdidas de información en caso de caída de uno de estos.

3.2 Alta disponibilidad

Una de las conclusiones a las que se ha llegado con el análisis realizado del estado de la red inicial es que, el grado de criticidad que tiene FDF en algunos puntos es muy alto y se debe rediseñar el sistema para obtener un estado de alta disponibilidad que ofrezca mayor robustez y fiabilidad a éste.

3.2.1 Topología de la red

En el estado inicial de FDF el sistema estaba demasiado distribuido ya que en todas las sedes existían servidores de recepción a través de los módems de 56kbps. Posteriormente se comenzó a instalar en la delegación de Barcelona los servidores de recepción de pedidos por ADSL, los cuales conforme fue pasando el tiempo fueron recibiendo la mayor parte del tráfico de pedidos El hecho de centralizar la mayor parte del tráfico de pedidos en un único punto de la red, resultaba muy crítico para el nivel de servicio que se tiene que dar.

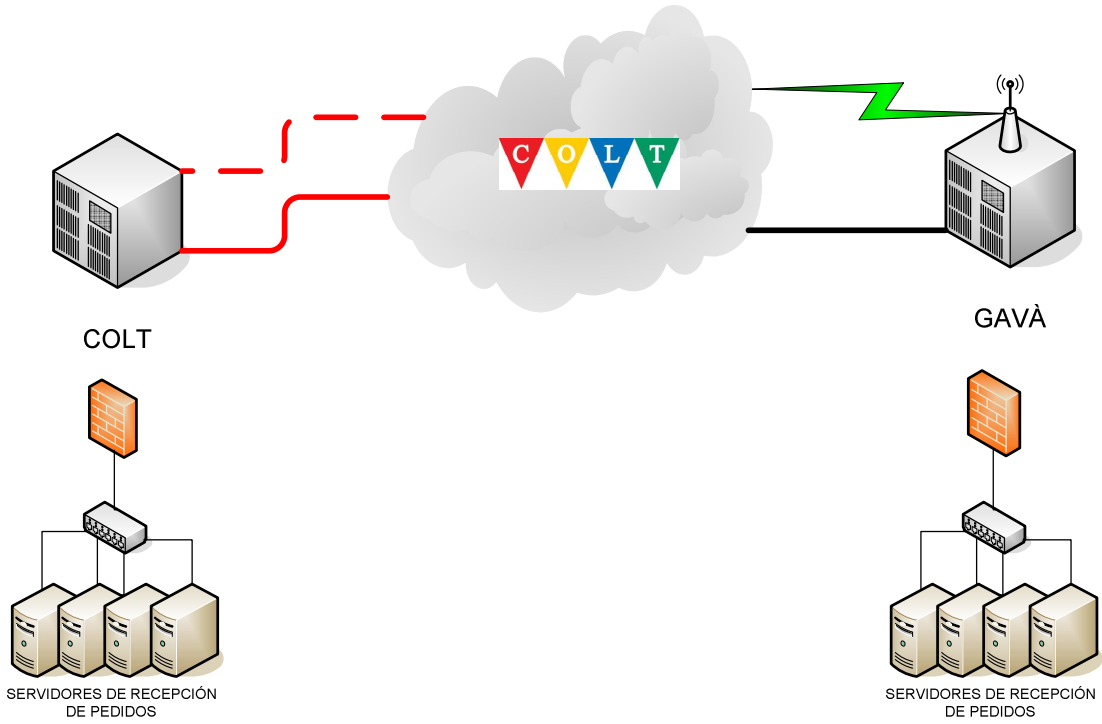


Fig. 3.4 Solución alta disponibilidad para la recepción de pedidos

Por este motivo se ha modificado la topología de la red. El diseño que se ha propuesto ahora, es repartir este volumen de tráfico en dos puntos (**Fig. 3.4**). De esta forma separamos los servidores que se encargan de la recepción de los pedidos. La topología de la red pasa a ser más distribuida y deja como puntos importantes el CPD de COLT y la nueva sede en Gavà.

Quisiera comentar que aún se siguen recibiendo pedidos a través de módems para las OF que mantienen este sistema de comunicaciones, el RACK (véase **Anexo 6.2**) de módems se encuentra ubicado en la delegación de Gavà.

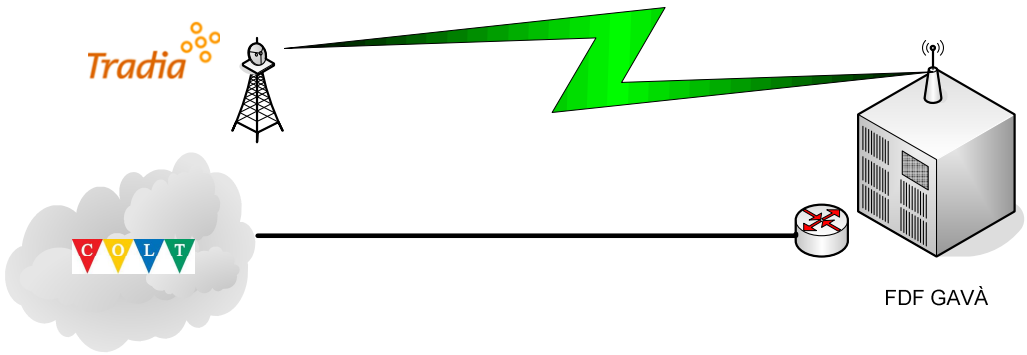
3.2.2 Enlaces WAN

Otro punto en el que se tuvo en cuenta la falta del concepto de alta disponibilidad fue en las comunicaciones de la WAN. Las sedes para comunicarse entre ellas usan la *MPLS* del proveedor de servicios contratado (inicialmente Telefónica).

La primera decisión que se tomo en este aspecto fue la de cambiar de proveedor de servicios, Telefónica no daba muestras de profesionalidad con una empresa "pequeña" como es FDF y se buscaron alternativas que mostraran más implicación con el proyecto que se estaba forjando.

Al-pi, ONO, entre otras; fueron opciones que se barajaron, aunque finalmente se decidió por COLT debido a la relación calidad – precio ofrecida y el tiempo de implementación del sistema que nos daba, a parte de dar un trato más personal y cercano que en el caso de Telefónica.

Una vez tomada esta decisión, se buscó poner una solución a la criticidad de tener un único medio de transmisión en la comunicación con las sedes a la MPLS (recordamos que el único medio de transmisión que existe inicialmente es el par de cobre). La solución fue diseñar un esquema de tierra-aire para todas las comunicaciones



.

Fig. 3.5 Esquema Tierra – Aire para las sedes

Un diseño de tierra-aire en el ámbito de las comunicaciones viene a referirse a un diseño en el que convivan las transmisiones aéreas (por radiofrecuencia: radioenlaces) y terrestres (a través de cable: ADSL, fibra,…) con el fin de que los enlaces de la mayoría de sedes tengan una vía alternativa en el caso de que uno de los dos medios fuera inutilizable.

En el caso de que se sucediese algún tipo de imprevisto en el que se viera afectado el enlace terrestre (por ejemplo causado por la realización de alguna obra pública) la sede no se quedaría incomunicada al encontrarse la vía aérea.

A parte se consigue dar mayor robustez a la comunicación de radioenlace gracias a que COLT contrata el servicio a través de otro proveedor, Tradia; ya que COLT no proporciona este tipo de comunicaciones. De esta manera la comunicación a la MPLS no depende en exclusiva a COLT.

3.3 Balanceo de Servicios

Como se ha comentado durante el estudio, FDF disponía de una serie de servidores repartidos entre sus sedes, y sus dos *DMZ (*véase **Anexo 6.2***)* colocados en la sede principal de Barcelona. En el estado inicial, la opción de acceder a un servidor u otro, era escogida manualmente por el usuario, accediendo a el a través de su nombre o su dirección IP.

Esto podía provocar que uno de los servidores se encontrara totalmente cargado, mientras que el resto no estaban dando servicio. Además, el usuario detecta el momento de caída de un servidor, ya que cuando uno de ellos está caído, si el usuario intenta acceder a él, se encontraría con el mensaje de error, esto de cara al socio puede provocar dudas (esto sucedía en el acceso a los servidores WEB)

Para evitar esto, se han colocado una serie de balanceadores de servicios delante de estos servidores, y de esta forma se tiene la opción de repartir cargas de trabajo, esconder las caídas de un servidor a los usuarios, etc.

Un **balanceador de carga (Fig. 3.6)** fundamentalmente es un dispositivo de hardware o software que se pone al frente de un conjunto de servidores que atienden una aplicación y, tal como su nombre lo indica, asigna o balancea las solicitudes que llegan de los clientes a los servidores usando algún algoritmo.

Estos balanceadores siempre tienen un secundario de back-up en caso de fallo del principal buscando la alta disponibilidad.

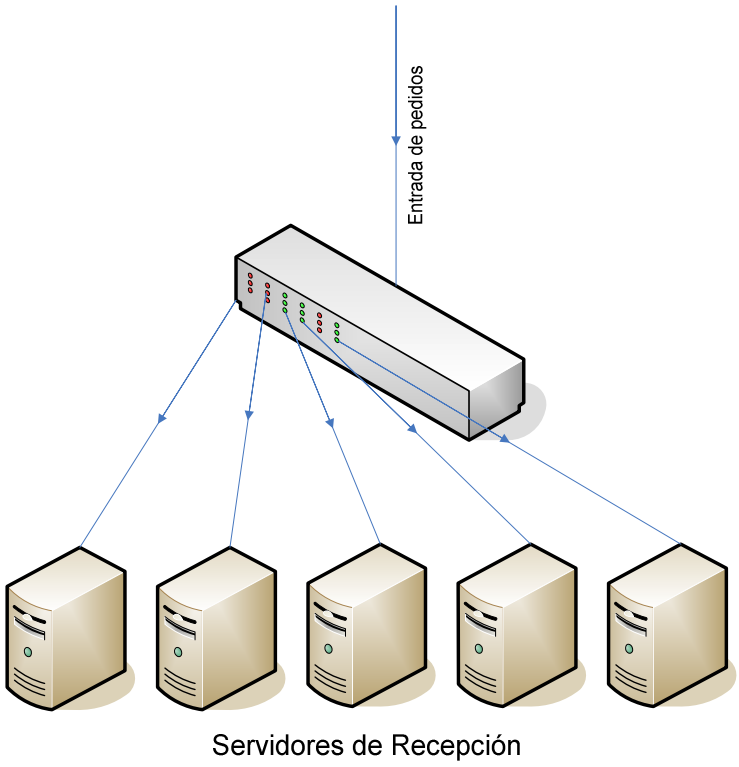


Fig. 3.6 Balanceo de carga en el servicio de recepción de pedidos

3.4 Cambio de hardware

Uno de los aspectos que han hecho mejorar el rendimiento de todo nuestro sistema de comunicaciones ha sido sin duda el cambio de hardware.

Se ha realizado una fuerte inversión en este aspecto, switches, routers, cableado, servidores, Firewalls,… se ha procurado renovar todo aquello que estaba obsoleto.

En este aspecto también se han barajado diferentes marcas, entre ellas Nortel, pero el mercado manda y hoy en día el mundo de las comunicaciones esta basado en CISCO.

También podemos comentar que el administrador de redes que tiene FDF posee ciertas certificaciones en CISCO y esto hizo que él mismo recomendará utilizar este fabricante.

El material instalado va desde firewalls *Cisco ASA* 5505 *(*véase **Anexo 6.2***)* con alta disponibilidad, por lo tanto, si uno de los dos dejase de funcionar el almacén continuaría trabajando sin ningún problema. Esto es gracias al protocolo HSRP comentado anteriormente.

También se podría dar que provocado por error en el enlace en los puertos de los firewalls constantemente estuvieran haciendo *failover (*véase **Anexo 6.2***)*; la solución sería apagar uno de los dos.

Los switches de usuarios *Cisco Catalyst* 2960-24/48TC-L a nivel de enlaces están redundantes y en caso de uno de los switches dejase de funcionar en todos los almacenes existe uno de back-up.

Por último hacer referencia a los switches *Core Cicsco Catalyst* 3750G-24TS *(*véase **Anexo 6.2)** también están en alta disponibilidad, por lo tanto, si uno de los dejase de funcionar el almacén continuaría trabajando sin ningún problema.

Para una visión más detallada del nuevo hardware implantado véase **Anexo 6.1**

3.5 Monitorización

Una vez implementadas las mejoras propuestas el nivel de rendimiento de la red aumenta considerablemente, evidentemente, se mejoraría el funcionamiento de la red, pero aumentarían los posibles elementos de fallo, que pudiesen provocar un problema en el funcionamiento de la estructura.

Para conseguir controlar con mayor detalle todos los elementos de red, es conveniente realizar el estudio de la viabilidad de implantar un sistema de monitorización en la red que nos permita conocer el estado actual de funcionamiento de los elementos más importantes de la misma.

Las posibles soluciones podrían ir desde soluciones gratuitas como Nagios, Cacti, etc., hasta otras con implicaciones económicas como *Sitescope*, *HP Openview*, etc.

En este caso se optó por la monitorización más económica y se han utilizado las herramientas Nagios y Cacti.

3.5.1 Nagios

Nagios es un sistema de monitorización de redes ampliamente utilizado, que vigila los equipos (hardware) y servicios (software) que se especifiquen (**Fig. 3.7**), alertando cuando el comportamiento de los mismos no sea el deseado. Entre sus características principales figuran la monitorización de servicios de red (SMTP, POP3, HTTP, SNMP...), la monitorización de los recursos de sistemas hardware (carga del procesador, uso de los discos, memoria, estado de los puertos...), independencia de sistemas operativos, posibilidad de monitorización remota mediante túneles SSL cifrados ó SSH.

Se trata de un software que proporciona una gran versatilidad para consultar prácticamente cualquier parámetro de interés de un sistema, y genera alertas, que pueden ser recibidas por los responsables correspondientes mediante (entre otros medios) correo electrónico y mensajes SMS, cuando estos parámetros exceden de los márgenes definidos por el administrador de red.

Nagios fue originalmente diseñado para ser ejecutado en Linux, pero también se ejecuta bien en variantes de Unix.

Nagios está parametrizado para que salten las alertas con diferentes niveles, dependiendo de la criticidad. Por ejemplo, si el router de Terrassa supera los 15ms de latencia saldrá una alerta, pero si se trata de Valencia, como la latencia es superior no tendremos una alarma hasta que la latencia supere los 40 ms.

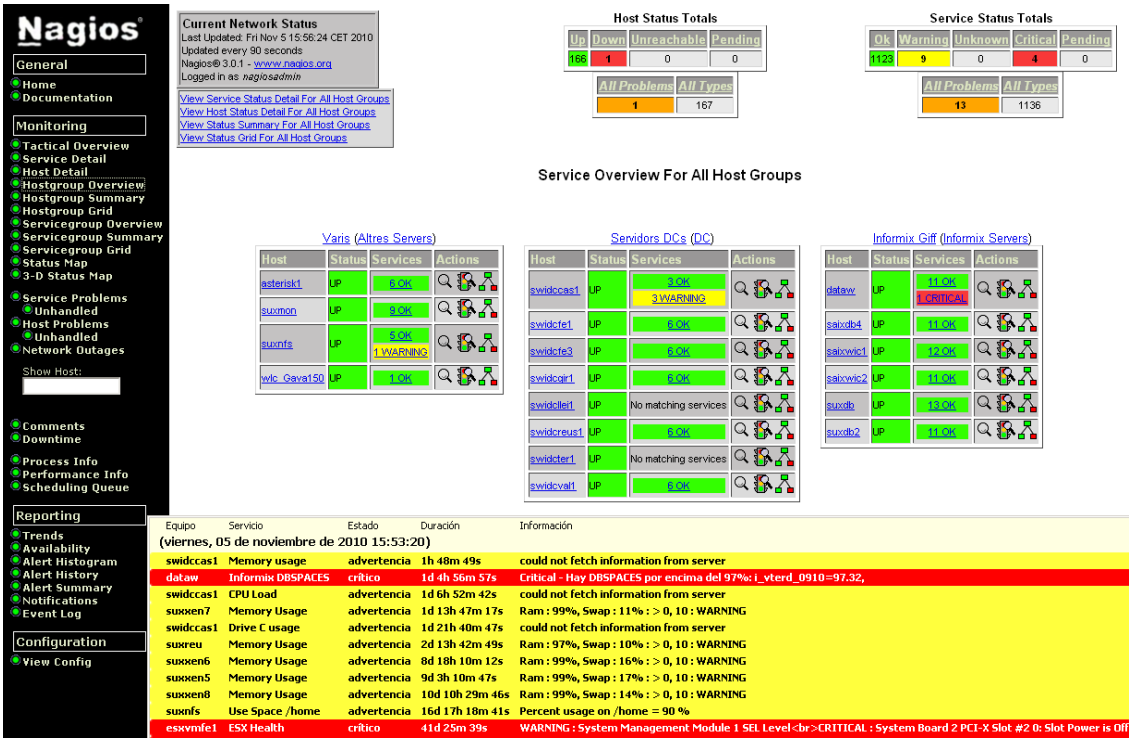


Fig. 3.7 Vista principal de servidores de la FDF monitorizado por Nagios

3.5.2 Cacti

Cacti (**Fig. 3.8**) es un programa de graficado en red, diseñada para aprovechar el poder de almacenamiento y la funcionalidad de graficar que poseen las *RRDtool (*véase **Anexo 6.2***)*. Esta herramienta, desarrollada en PHP, provee plantillas de gráficos avanzadas, múltiples métodos para la recopilación de datos, y manejo de usuarios.

Tiene una interfaz de usuario fácil de usar, que resulta conveniente para instalaciones del tamaño de una LAN, así como también para redes complejas con cientos de dispositivos.

Dadas las muchas funciones que ofrece Cacti, la herramienta cuenta con la funcionalidad de manejo de usuarios, para así hacer posible agregar un usuario y darle permisos a ciertas áreas de Cacti.

Esto permite tener usuarios que puedan cambiar parámetros de un gráfico, mientras que otros sólo pueden ver los gráficos. Asimismo, cada usuario mantiene su propia configuración de vista de gráficos.

En Nagios las alertas nos llegan cuando sea el caso, pero Cacti es una herramienta en la cual se tiene que estar consultando ya que la información que nos da son tendencias de uso de los servidores, comunicaciones, primarios, centralitas, etc.

Si se quiere ser proactivo *(*véase **Anexo 6.2***)* hemos de consultar los diferentes elementos para ver si nos estamos aproximando al número máximo de

conexiones concurrentes en un firewall, o estamos saturando la línea de comunicaciones que da acceso a nuestros servidores en Colt, o tenemos muchos errores de CRC en un puerto de un switch.

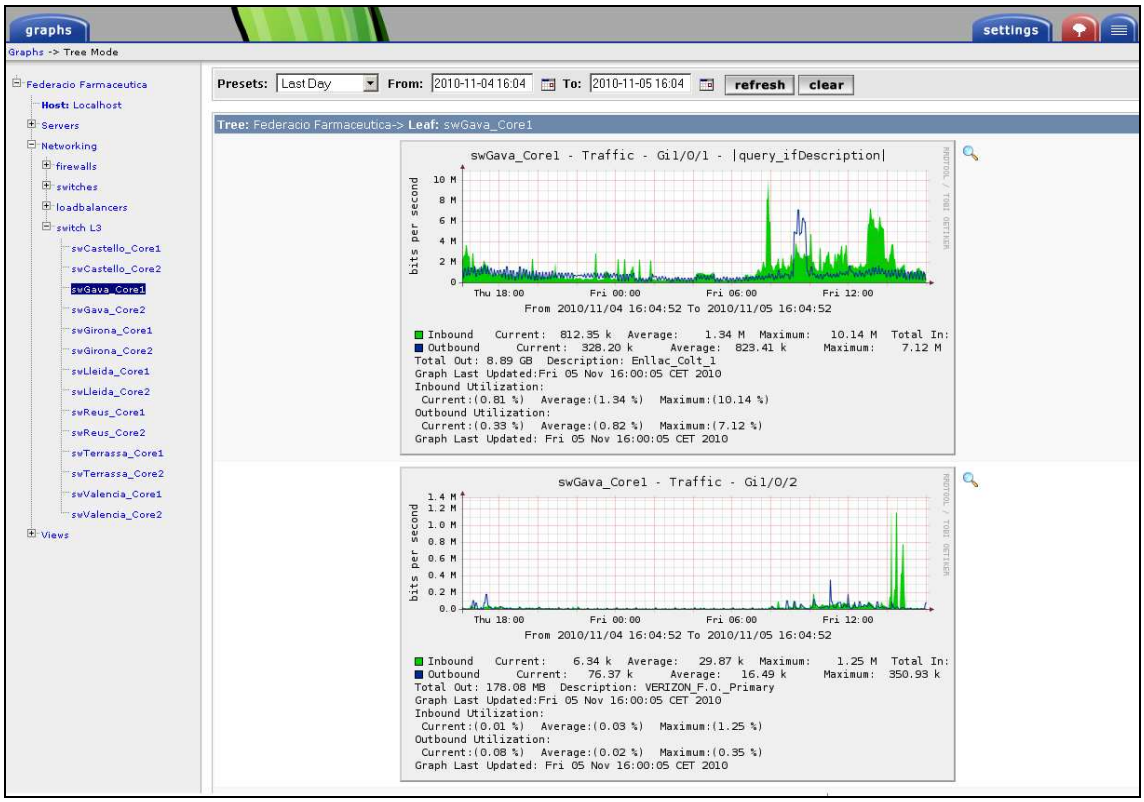


Fig. 3.8 Vista de tráfico de las entradas en el *Core* de Gavà de Cacti

3.6 Priorización de tráfico

Antes de nada querría comentar que el tema que menciono a continuación aún está en su fase inicial, pero aunque aún deben pasar unos meses para que se implemente al 100%; considero que es un punto importante ya que repercutirá en la mejora de calidad de ciertos servicios.

Uno de los proyectos que están pendientes de ponerse en marcha es el de la priorización del tráfico.

La finalidad de este proyecto es ofrecer más recursos de transmisión al tráfico que se considere prioritario para conseguir una mayor calidad de servicio para éste en reprimenda del resto.

Para FDF el tráfico prioritario por delante de todo es el tráfico que generan los pedidos realizados por los socios, por lo que se proporcionará el ancho de banda que requiera. Luego existen muchos tipos de tráfico comentados en apartados anteriores que aún están pendientes de determinar su grado de importancia para darles el grado prioritario correspondiente.

En próximos proyectos de FDF están previstos implementar la VoIP (Voz sobre IP) para las llamadas internas de la empresa así como un servicio de Video *Streaming* (véase **Anexo 6.2**) para realizar conferencias on-line para las OF. Estos servicios tendrán que tener una reserva previa de tráfico para obtener una alta calidad de estos.

Gracias al nuevo hardware CISCO implementado podremos configurar estos parámetros. Está previsto que la fase inicial de la implementación de esta mejora dé comienzo durante el tercer o cuarto trimestre de este año.

4. RESULTADOS Y CONCLUSIÓN

Des de que se inició este proyecto han transcurrido más de dos años durante los cuales se han ido implementando las mejoras propuestas en el capítulo anterior (a excepción de la priorización de tráfico, como ya recalcamos anteriormente). Llegados a este punto, se puede realizar un análisis de los resultados obtenidos en la actualidad y realizar una comparación de algunos puntos con el estado inicial de la red.

A priori se puede comentar que los resultados obtenidos han sido positivos y se ha conseguido mejorar la calidad del servicio cumpliendo es esta manera el objetivo principal.

De la misma forma también cabe comentar que nos hemos encontrado también ciertos problemas con algunas de las mejoras implementadas y que en un futuro deberán ser replanteadas debido al rendimiento final que nos están dando.

4.1 Pedidos y Tiempo de espera

Para empezar realizamos una comparativa gráfica (**Fig. 4.1**) de los pedidos que se han recibido durante el transcurso de la implementación de las mejoras.

En este punto cabe aclarar que los datos que se muestran a continuación han sido adquiridos de la base de datos de FDF (véase **Anexo 6.3**).

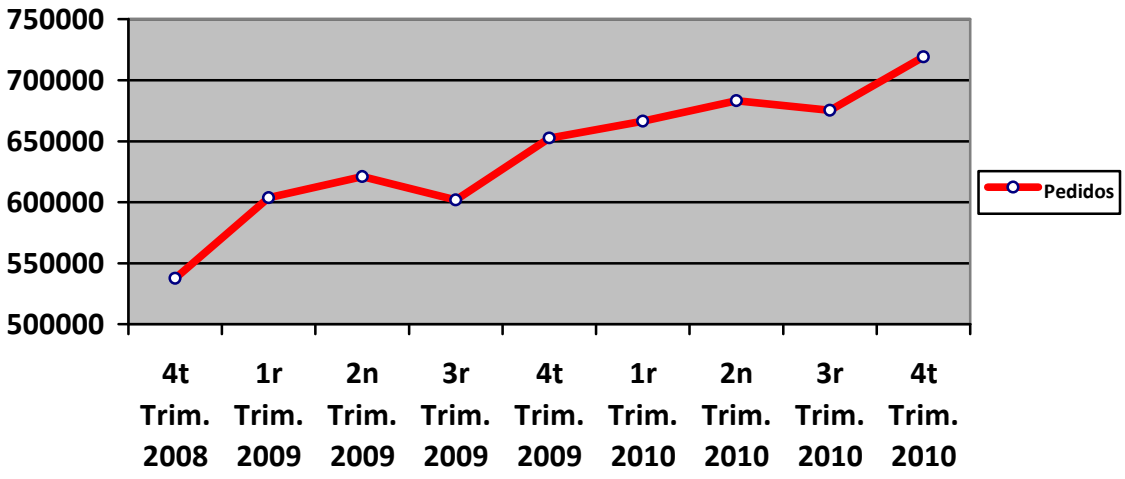


Fig. 4.1 Evolución de la demanda de pedidos a FDF los últimos trimestres

Desde que comenzamos a implementar las mejoras hasta el día de hoy hemos pasado de recibir 537.638 pedidos durante el transcurso del último trimestre del 2008 a recibir 719.096 pedidos en el mismo trimestre de 2010.

De esta manera se ha logrado aumentar el volumen de pedidos un 33,7% en el transcurso de dos años, lo que se ha considerado una mejora notable para el crecimiento de FDF.

Por último comentar de esta gráfica que la razón de que haya un descenso del número de pedidos durante el tercer trimestre de ambos años es debido a la llegada del periodo vacacional, lo que repercute en el cierre temporal de muchos de nuestros socios. Por lo demás la gráfica siempre muestra un comportamiento creciente en todo el periodo.

Otro aspecto que se puede observar para valorar la mejora del rendimiento de nuestro sistema, es en el tiempo de espera que tiene el pedido hasta entrar en éste. Este tiempo de espera comienza en el momento en el que el socio realiza la petición hasta que el pedido se inserta en nuestra base de datos. En la **Fig. 4.2** se puede ver la evolución trimestral que se ha dado desde finales del 2008 hasta ahora en el periodo crítico de recepción de pedidos del mediodía.

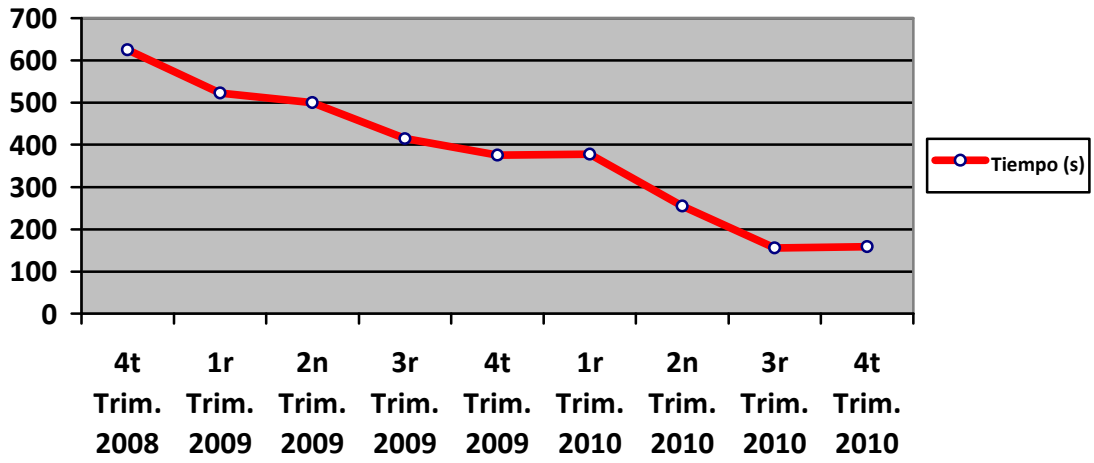


Fig. 4.2 Evolución del tiempo de espera de un pedido en media de 13h a 15h

En la **Fig.4.3** observamos el otro periodo crítico diario de 19 a 21 horas, para el cierre de las OF.

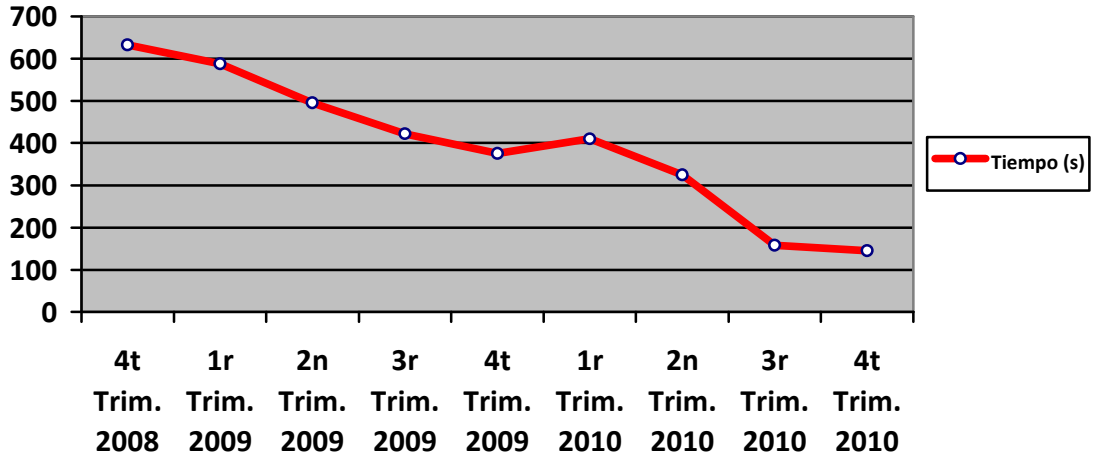


Fig. 4.3 Evolución del tiempo de espera de un pedido en media de 19h a 21h

En las dos gráficas podemos observar el significativo descenso del tiempo de espera que se han dado en los dos tramos horarios. Se ha pasado de un tiempo de espera medio de 10 minutos a los 90 segundos que hay de media en la actualidad.

El periodo de tiempo mostrado en las gráficas se inicia en el momento que el socio realiza el pedido y finaliza cuando nuestros sistemas insertan el pedido en nuestra base de datos.

En medio de este proceso el pedido se transfiere por nuestro sistema de comunicaciones hacía los servidores de recepción. Aquí tienen que esperar a entrar en el servidor mientras se procesan otros pedidos (este es el tiempo más importante en el proceso) y finalmente cuando el servidor atiende la solicitud de este pedido, lo procesa e inserta en la base de datos.

La mayor parte de la mejora de todo este proceso viene dada al aumento de servidores de recepción y la descentralización de esta. Inicialmente se concentraban 6 servidores de recepción en la sede de Barcelona mientras ahora se reparten 13 servidores entre la sede de Gavà y el CPD de COLT *(*véase **Anexo 6.2***)*.

Esto es un hecho realmente importante, más teniendo en cuenta el aumento de pedidos, y más aún que este hecho en sí mismo, porque; una de las múltiples quejas que tenían los socios es que su pedido no llegaba en el reparto que tocaba (FDF dispone de cuatro repartos diarios). Esto era a causa de que debido al tiempo de espera que había anteriormente cuando llegaba a entrar el pedido en el sistema la hora de su reparto había pasado. De esta manera se ha conseguido dar un importante salto en la calidad de servicio que se ofrece al socio.

4.2 Enlaces

A continuación se expone un análisis del estado de los enlaces estudiados en el estado inicial y se compara con el estado actual.

4.2.1 COLT – Gavà

A priori el consumo de tráfico que se observa en la **Fig. 4.4** es menor que en la **Fig. 1.7** pero cabe recordar que ahora el tráfico total de FDF se gestiona des dos puntos COLT y Gavà que es donde se encuentran los servidores.

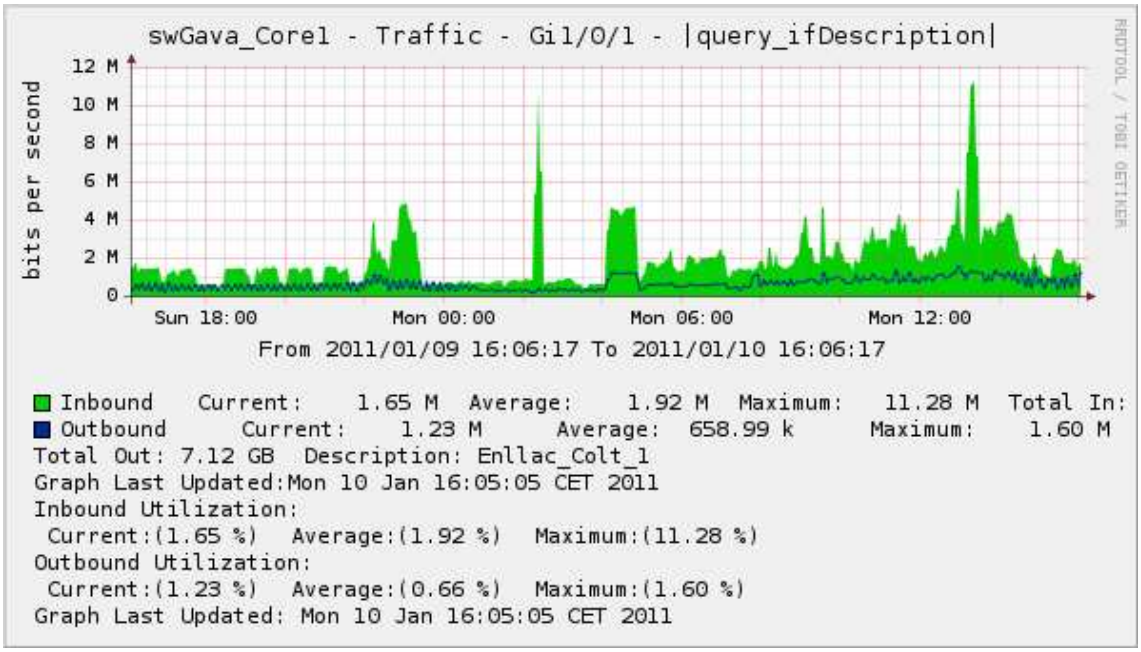


Fig. 4.4 Tráfico entrante y saliente del enlace Gavà – COLT a través del swGava_Core1 (enlace COLT)

Existen ciertas franjas horarias donde el tráfico aumenta considerablemente, durante el mediodía y última hora de la tarde se observa un incremento del tráfico considerable del cual la mayoría corresponde al tráfico generado por la recepción de pedidos. Esto lo podemos ver más claro en la **Fig. 4.5** donde hacemos un zoom de este periodo crítico.

Por otra parte durante tramos horarios nocturnos también vemos como se incrementa el tráfico en la delegación, esto es debido a procesos tales como copias de seguridad, traspaso de ficheros vía FTP para el control del stock del almacén, etc. que realizan otros de los servidores que se encuentran en el CPD *(*véase **Anexo 6.2***)* de la delegación.

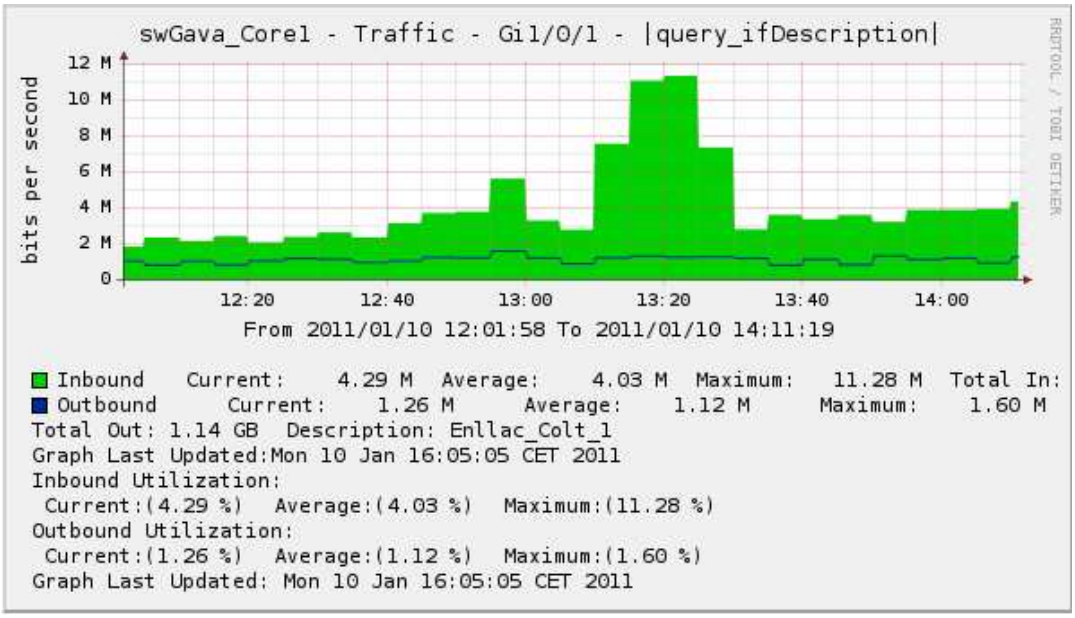


Fig. 4.5 Ampliación de la **Fig. 4.4** en el tramo horario de mayor tráfico

Por último se realiza una visión semanal del consumo de tráfico de la sede. Los días 8 y 9 corresponden al fin de semana donde se observa un descenso considerable de tráfico, así como el día 6, que corresponde al 6 de enero (festivo). El resto de días comparten el mismo patrón.

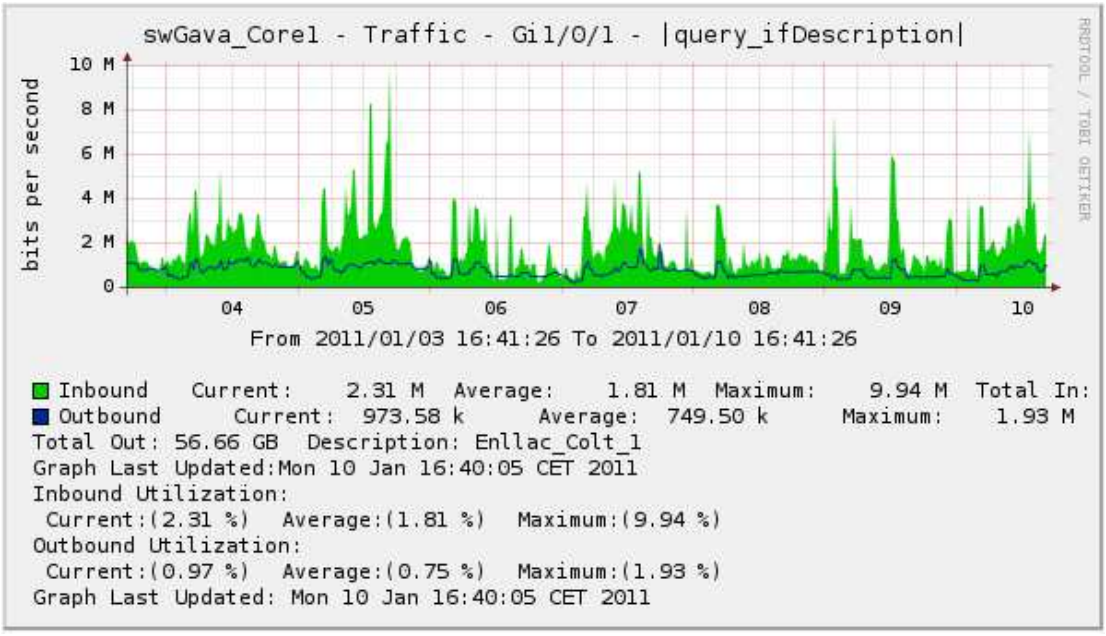


Fig. 4.6 Tráfico entrante y saliente del enlace Gavà – COLT durante el transcurso de una semana

4.2.2 COLT – Valencia

La **Fig. 4.7** muestra el tráfico registrado por la aplicación *Cacti* de la sede de Valencia en diferentes periodos de tiempo (Diario, Semanal, Mensual).

Antes de comentar los gráficos y compararlos con su estado inicial, cabe decir que por un problema en la configuración de Cacti, el eje de coordenadas no refleja el tráfico correcto. Esta dividido por un factor 100, por lo que debería reflejar de 2Mbps a 8Mbps.

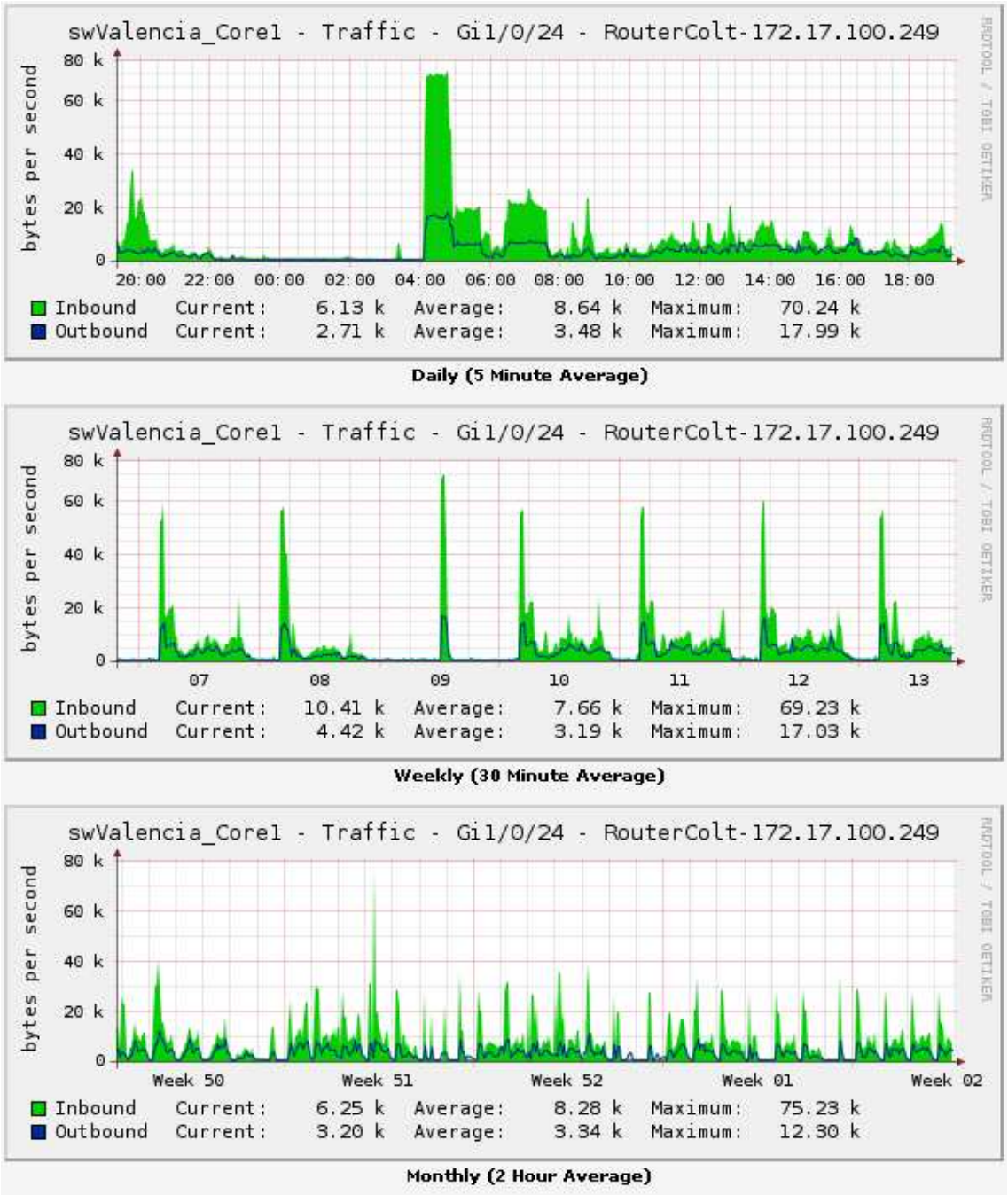


Fig. 4.7 Tráfico entrante y saliente en la delegación de Valencia a través del swValencia_Core1

Para comenzar recordaremos que el enlace que existe entre la MPLS de COLT y la sede de Valencia corresponde a 8Mbps (4Mbps de fibra óptica y 4Mbps de radio enlace).

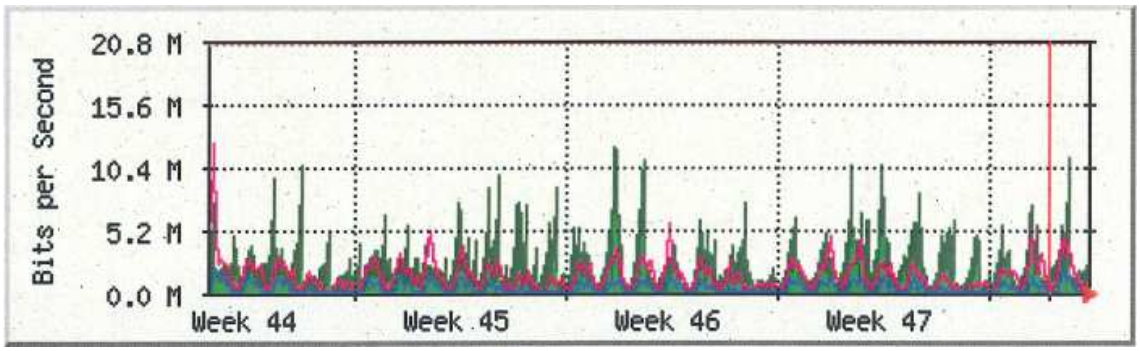
En la gráfica diaria, observamos con el consumo de tráfico se dispara considerablemente respecto al resto del día de las 4:30 a las 8:00 de la mañana que es cuando se lanza el proceso de actualización del stock de cada almacén, llegando a consumir aproximadamente el 87% del ancho de banda del enlace. El resto del día el tráfico se encuentra normalmente por debajo de los 2Mbps, solo vuelve a sobrepasarlo durante las horas críticas.

En la siguiente gráfica, correspondiente a la gráfica semanal; se puede observar como este proceso se realiza diariamente en el mismo rango horario siguiendo así un mismo patrón. Lo único que podemos destacar de esta gráfica es la variación de tráfico que existe en los días 8 y 9, correspondientes al fin de semana; debido a que el número de socios que solicitan nuestros servicios durante el fin de semana es muy bajo ya que muchos de estos no tienen abiertas sus OF.

Por último querría comentar de la gráfica mensual que se aprecia la repetición del mismo patrón diariamente y recalcar que en ningún momento se sobrepasa la totalidad del ancho de banda del enlace, solventado los problemas de capacidad que teníamos tanto en la entrada como en la salida de datos en el estado inicial (**Fig. 1.10**).

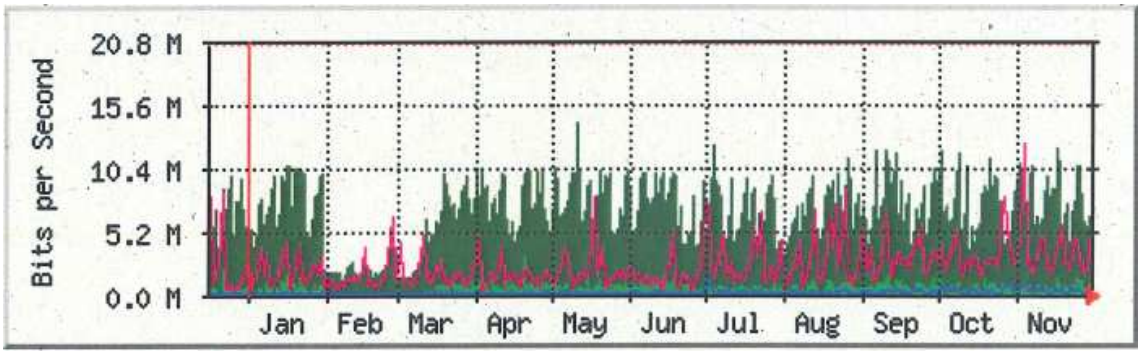
4.2.3 Internet – COLT

Las primeras gráficas que mostramos (**Fig. 4.8** y **Fig. 4.9**) hacen referencia al consumo de acceso a Internet que hay en *COLT.*



Max Entrante: 12,1Mbps (59%) Promedio Entrante: 887kbps (4,3%)
Max Saliente: 12,5Mbps (60,9%) Promedio Saliente: 394kbps (1,9%)

Fig. 4.8 Acceso a Internet *COLT* Noviembre 2010



Max Entrante: 14,3Mbps (69,7%)
Max Saliente: 12,5Mbps (60,9%)

Promedio Entrante: 794kbps (3,9%)
Promedio Saliente: 227kbps (1,1%)

Fig. 4.9 Acceso a Internet *COLT* Anual

Debemos tener en cuenta que en la **Fig. 4.8** y **Fig. 4.9** el ancho de banda entrante es el tráfico saliente de la plataforma y viceversa.

Como se puede observar, el tráfico de pico excede los 4 Mbps tanto en lo que refiere a al entrada como a la salida. Gracias a que el servicio contratado nos permite excedernos del ancho de banda contratado no tenemos problemas de pérdidas ni congestión en la línea (límite 20Mbps).

Habrá que analizar la tendencia en futuros meses para ver si este consumo se mantiene o sufre alguna variación ya que el exceso del consumo del ancho de banda contratado se verá reflejado en la facturación del servicio. En ese caso se debería plantear si es conveniente la contratación de más ancho de banda o no.

No existen referencias anteriores a estas gráficas en el estado inicial pero parece interesante comentar este punto ya que es la entrada directa de los pedidos de los socios, así como, las conexiones de estos a la web de FDF además de otros servicios.

4.3 Rendimiento LAN

En el análisis inicial se vio como el rendimiento de la red local de nuestras sedes era bastante bajo. Después de realizar todos los cambios comentados como el cambio de hardware, cableado,… se ha hecho un análisis de las estadísticas actuales en los puertos que fueron anteriormente chequeados.

En el primer caso se compara la **Fig. 4.10** con la **Fig. 2.11**, en el estado inicial el porcentaje de tramas broadcast que recibíamos por este puerto era del 9,7%, en la actualidad podemos observar como este porcentaje ha descendido a un 0,42%.

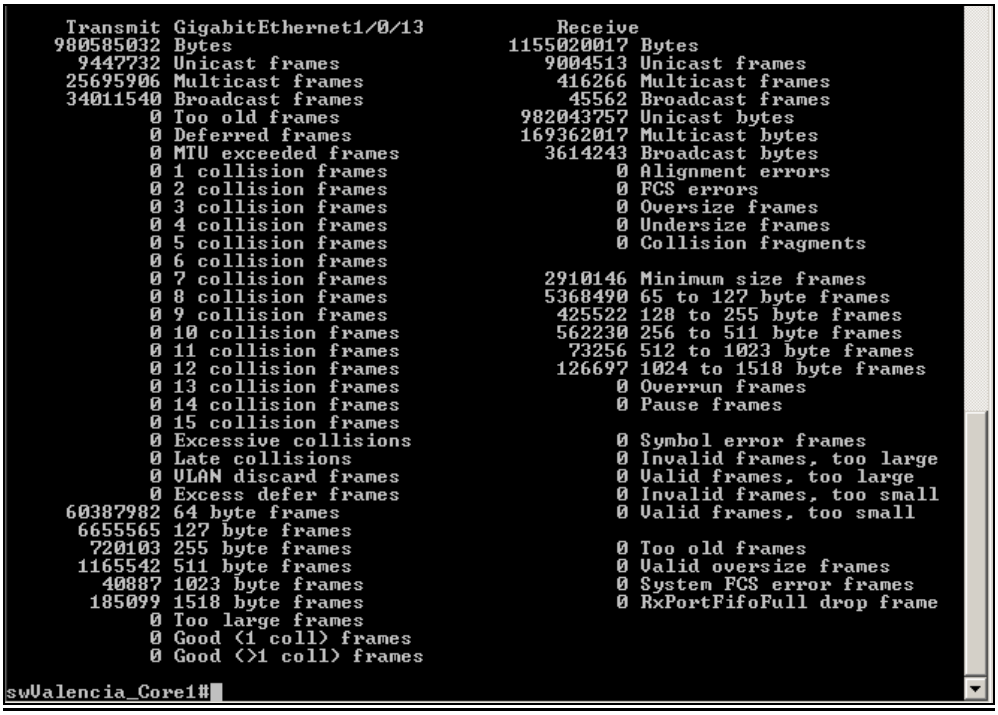


Fig. 4.10 Estadística de las transmisiones y recepciones del puerto 13 del switch principal de la delegación de Valencia

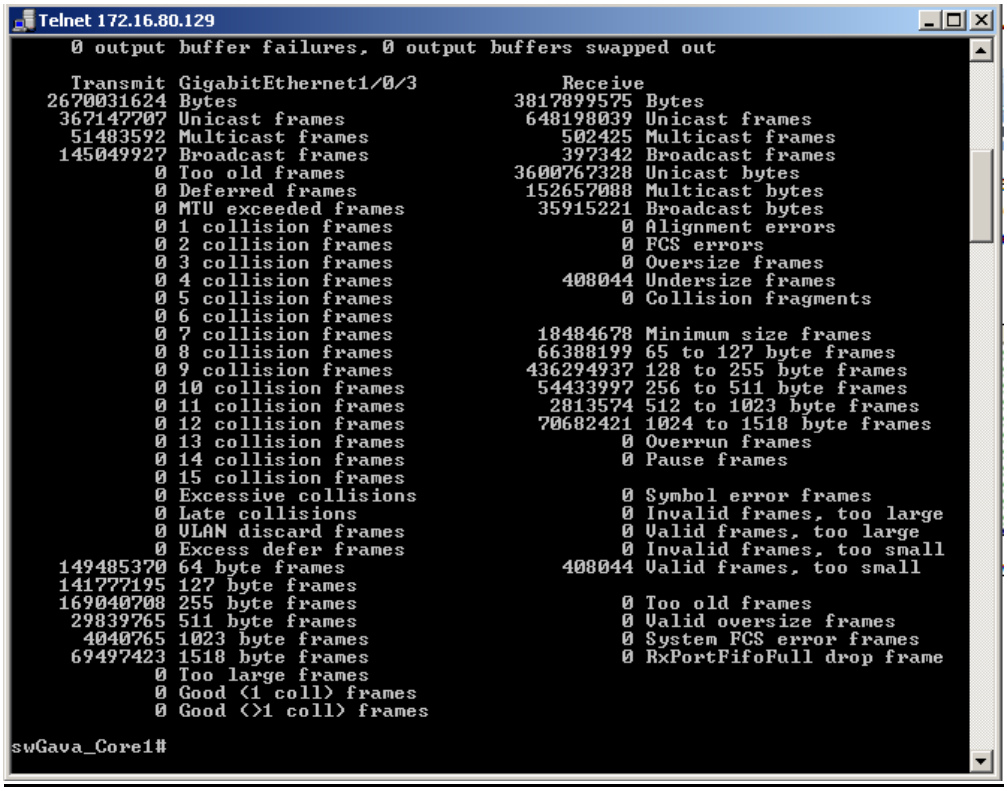
En Lleida en cambio observamos como el registro de estadísticas del switch nos informaba de que el número de colisiones era de 243.000 (**Fig. 2.13**) mientras que por lo que lleva registrado por el momento el nuevo hardware es de 0 colisiones (**Fig. 4.11**). Los elementos de red no gestionables provocaban un deterioro importante de la red.

Fig. 4.11 Estadística de las transmisiones y recepciones del puerto 24 del switch principal de la delegación de Lleida

Para finalizar con este apartado recordamos en el análisis inicial las características dadas en la sede de Barcelona. En esta sede que en aquel momento la sede principal, se registro en su red interna un 10% de tráfico broadcast (**Fig. 2.9**). Ahora la sede principal se encuentra en Gavà como hemos comentado y recogiendo estadísticas de los puertos principales de conexión podemos realizar una comparación para ver si hemos logrado bajar este porcentaje.

Realizamos capturas del Switch_Core_Gava1 de sus puertos 3 y 5 (**Fig. 4.12**) donde se encuentran conectados la mayor parte de usuarios a través de los switches secundarios.

Haciendo cálculos se obtiene que de estas capturas (**Fig. 4.12**) el porcentaje que se registra de tramas broadcast corresponde al 0,02%, lo que muestra una muy significativa mejora del rendimiento de la red interna de Gavà.



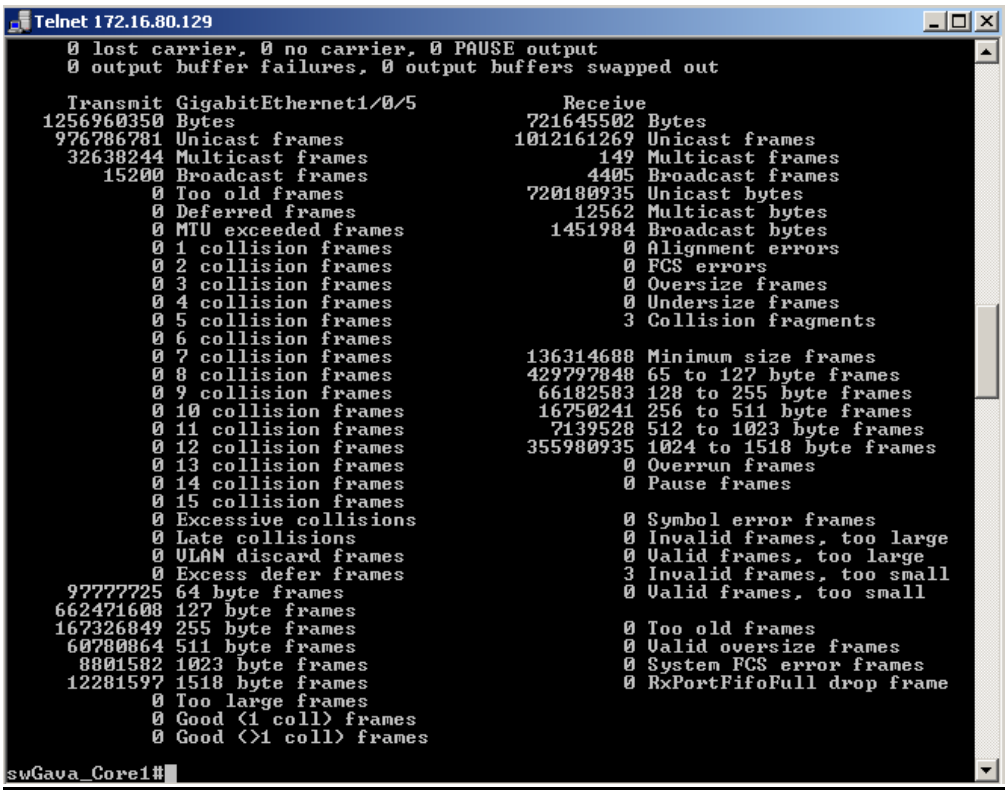


Fig. 4.12 Estadísticas de las transmisiones y recepciones de los puertos 3 y 5 (**Fig. 2.8**) del switch principal de la delegación de Gavà

4.4 Calidad del ISP – COLT

Uno de los puntos en los que hemos tenido que poner mucha atención es en el nivel de calidad que proporciona nuestro nuevo proveedor de comunicaciones, COLT. Mensualmente se nos envía un informe donde nos reflejan el nivel de servicio ofrecido.

El servicio que nos hemos encontrado es de alta calidad, la mayor parte de los meses la eficiencia del servicio es del 100%.

La disponibilidad de la MPLS (en los enlaces de los que se dispone información) indica un nivel de eficiencia superior al 99,7%. En la **Fig. 4.13** se muestra una gráfica donde se observa el nivel de calidad que ofrece COLT en el último semestre del 2010.

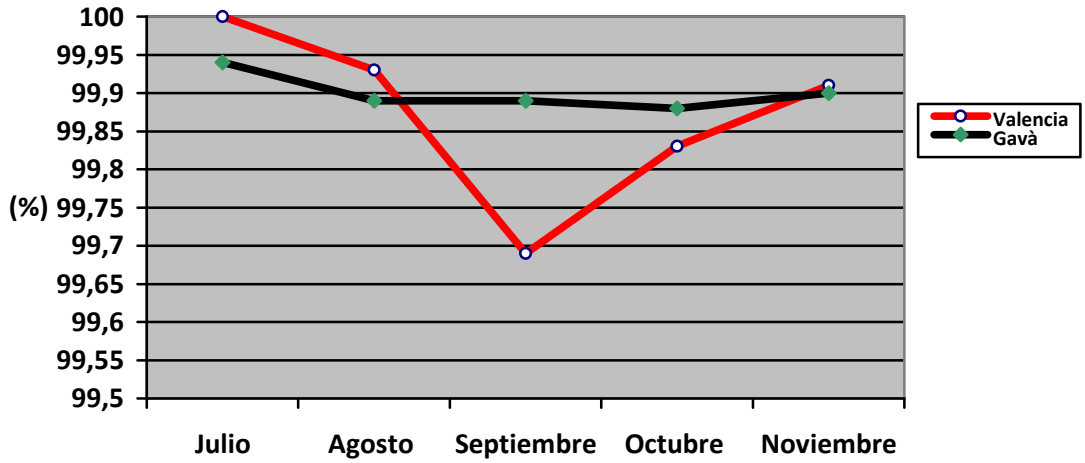


Fig. 4.13 Disponibilidad de los enlaces de Valencia – Colt y Gavà – Colt

Aun así, existe un punto débil en la comunicación ofrecida por este proveedor. Las pocas incidencias que hemos tenido se han debido a la caída del circuito del enlace de comunicaciones por algún problema en algún puerto. De nada sirve que tengamos la línea de back-up ya que la comunicación aérea como terrestre usa el mismo circuito.

Para evitar este imprevisto se debería contratar que cada medio de comunicación use circuitos diferentes, de esta manera el back-up sería completo, aunque el coste incrementaría considerablemente. Por esta razón y debido a la fiabilidad del sistema de COLT se mantiene el mapa actual y no se realizará ninguna modificación por el momento.

A continuación se muestra el histórico de incidencias que se han ido sucediendo durante el transcurso del 2010, y el tiempo de resolución que ha tenido COLT de estas:

Mes	Nº Inc. Críticas	MTTR Crítico	Nº Inc. Altas	MTTR Alta	Nº Inc. Media	MTTR Media	Nº Inc. Baja	MTTR Baja
Febrero	0	0	3	33.46	1	24.25	20	49.74
Marzo	0	0	1	13.14	0	0	2	66.62
Abril	0	0	0	0	0	0	0	0
Mayo	0	0	1	5,17	0	0	2	20.68
Junio	0	0	2	19.32	0	0	1	141.22
Julio	0	0	1	117.82	3	67.49	1	0.64
Agosto	0	0	0	0	3	44.04	1	71.91
Septiembre	0	0	1	1.17	4	5.97	3	15.65
Octubre	0	0	1	16.24	2	22.45	2	16.83
Noviembre	0	0	1	0.93	1	4.13	2	73.73

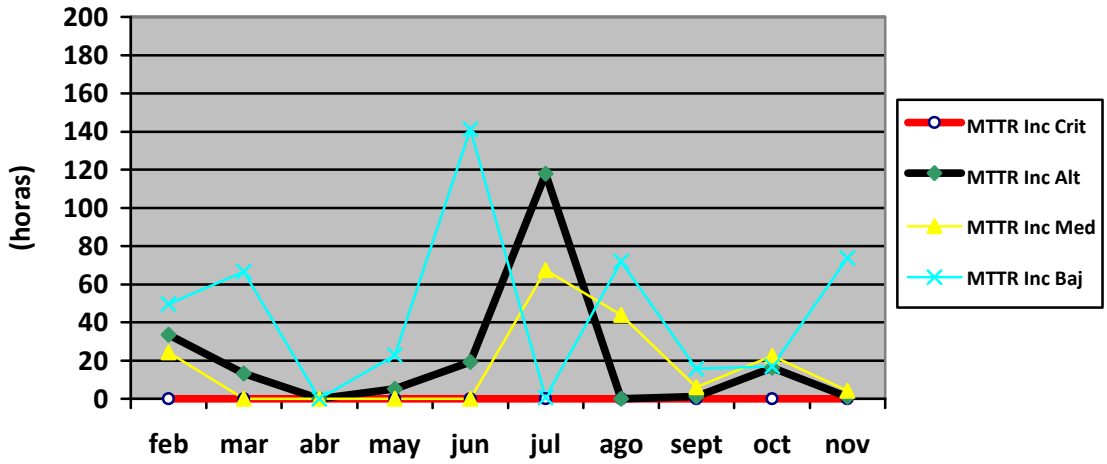


Fig.4.14 Análisis del MTTR durante el 2010

El MTTR (*Mean time to Recovery*) en el cual hacemos referencia en la tabla y gráfica anterior (**Fig. 4.14**), es el tiempo medio que se necesita para recuperarse de un error, en este caso nos referimos a los enlaces de la MPLS. Las unidades de esta variable son horas.

El tipo de incidencias con las que normalmente nos podemos encontrar son caídas del circuito de algún enlace, aunque en alguna ocasión también se han abierto *tickets* por degradación de enlace.

Respecto al uso del ancho de banda de la MPLS comentar que no hay problemas de capacidad. El uso está por debajo del ancho de banda contratado, aunque los enlaces de algunas sedes presentan picos de tráfico con valores superiores al 90% que sería conveniente analizar para ver si es necesario ampliar la capacidad de la línea (**Fig. 4.7**).

4.5 Conclusiones Finales

En esta última sección se realiza un análisis general de todo el proyecto y extrae conclusiones del mismo.

Lo que ha supuesto este proyecto de renovación tecnológica para FDF, ha sido ante todo el hecho de volver a ser competitivos en el mercado de la distribución de fármacos, se ha logrado aumentar la calidad del servicio ofrecido considerablemente y como consecuencia; se ha aumentado la demanda de pedidos como se ha comentado anteriormente (ver **Fig. 4.1**)

El motivo del aumento de la calidad del servicio se ha dado gracias, principalmente a dos puntos:

- La eliminación de las carencias que se padecían (ancho de banda insuficiente en algunos enlaces, hardware obsoleto, …)
- El concepto de “Alta disponibilidad” que se ha desarrollado en el proyecto.

Las consecuencias de esta mejora no se están haciendo esperar ya que se están buscando nuevos clientes en otras zonas geográficas de la península sin la necesidad de abrir nuevos almacenes. El almacén principal en Gavà se encargaría de darles soporte. El hecho de disminuir el tiempo de recepción del pedido ofrece un mayor margen horario para poder plantearse esta distribución a grandes distancias.

Paralelamente se están realizando otros proyectos donde se pretende dar nuevos servicios a los socios:

- Aplicativos para móviles (desde donde los socios pueden realizar sus pedidos)
- Seguridad en las OF a través de cámaras IP

En términos generales el balance ha sido muy positivo para FDF y ahora el reto que se tiene es no caer de nuevo en el mismo error e ir renovando nuestros sistemas constantemente.

5. BIBLIOGRAFÍA

La mayor parte de la documentación usada para realizar este proyecto ha sido proporcionada por el departamento de SSII de FDF. Aún así, para ciertos puntos teóricos del proyecto sobretodo; se ha usado la siguiente bibliografía:

- http://es.wikipedia.org/wiki/
- http://www.cacti.net/
- http://www.nagios.org/
- http://www.cisco.com/en/US/products/index.html
- http://aprenderedes.com
- http://www.colt.net/ES-es/index.htm

6. ANNEXO

6.1 Nuevo Hardware

A continuación mostramos el hardware que se ha implementado en todo el proyecto de FDF:

Cores y Switches repartidos en las diferentes delegaciones para la implementación de su red local.

Modelo	Unidades	Descripción
CON-CSSPP-3750GS1	14	CSS Cisco Catalyst 3750
CON-CSSPD-C29604T	30	CSS Cisco Catalyst 2960 48
CON-CSSPD-C29602T	1	CSS Cisco Catalyst 2960 24
CON-CSSPP-WC44022	2	CSS Cisco WLAN Controller 4400
CON-CSSPU-WCSSTD	1	CSS Cisco WCs Top Level SKU
CON-CSSPU-WCSAB5	1	CSS Cisco WCS 50 AP

Puntos de acceso LWAPP 125AG (Soporta estándares 802.11 a/g/n).

Modelo	Unidades	Descripción
AIR LAP 125 AG-E-K9	1	Cisco 802.11a/g/n
AIR ANT 2422 DB-R	3	Cisco 2.4GHz 2.2dB Antenna RP
AIR ANT 5135 DB-R	3	Cisco 5GHz 3.5dB Antenna RP
AIR PWINJ4	1	Cisco Power Injector 1250 Series
AIR AP1250MNTGKIT	1	Cisco 1250 Series Ceiling Wall Mount
S125RK9W-12410 JA	1	Cisco 1250 Series IOS Wireless LAN

En temas de seguridad se implementaron los siguientes dispositivos:

Modelo	Unidades	Descripción
ASA 5505	14	Cisco ASA Series 5500

6.2 Glosario

A

ASA: se trata de un dispositivo de seguridad de CISCO que admite la personalización de la seguridad según sus necesidades de acceso específicas y sus políticas comerciales, da seguridad de contenidos, cifrado, autentificación de identidad, autorización, prevención de intrusiones. A su vez se trata de un dispositivo fácil de instalar, administrar y supervisar.

C

Checkpoint: es una compañía de software de seguridad, conocida por sus firewalls y productos VPN. En este caso cuando nos referimos en el texto a Checkpoint nos referimos al Firewall que tenemos en Gavà.

Core: es un switch que provee de alta velocidad hacia tu *backbone* o puerto WAN estos switch debe manejar los paquetes tan rápido como sea posible, es el cerebro de tu red, recuerda que el *Core* es critico para la conectividad, esta capa maneja alto nivel de disponibilidad y debe adaptarse a los cambios que sufra tu red de manera inmediata.

CPD (Centro de procesamiento de datos): Ubicación donde se concentran todos los recursos necesarios para el procesamiento de la información de una organización. Se usa ara mantener en él una gran cantidad de equipamiento electrónico. Suelen ser creados y mantenidos por grandes organizaciones con objeto de tener acceso a la información necesaria para sus operaciones.

D

Diafonía: Se denomina diafonía al fenómeno que sucede entre dos circuitos existentes cuando parte de las señales presentes en uno de ellos, considerado circuito perturbador, aparece en el otro, considerado circuito perturbado. En el caso de los cables trenzados la diafonía se presenta generalmente debido a acoplamientos magnéticos (**Fig. 6.1**).

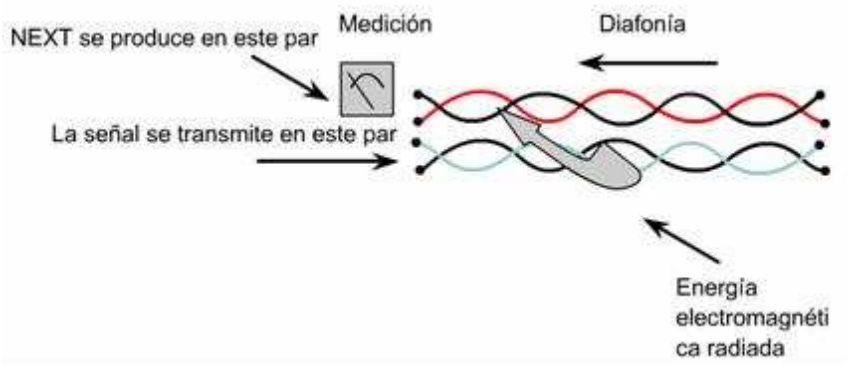


Fig. 6.1 Explicación del fenómeno de la diafonía

DMZ (Zona Desmilitarizada): esta “zona” es una red que se ubica entre la red interna de la empresa y una red externa, con el objetivo de que los equipos que se encuentren en esta red puedan dar servicios a la red externa, a la vez que protegen la red interna de intrusiones y ataques. La DMZ se usa habitualmente para ubicar servidores que es necesario que sean accedidos desde fuera, como servidores de correo electrónico, Web y DNS.

F

Failover: Modo de operación de back-up en el cual las funciones de un componente del sistema son asumidas por un segundo componente del sistema cuando el primero no se encuentra disponible debido a un fallo ó un tiempo de parada preestablecido. Es usado para hacer a los sistemas más tolerantes a fallos, y de esta forma hacer el sistema permanentemente disponible.

K

KNAPP: empresa que cubre todas las alternativas posibles de soluciones logísticas: desde la simulación hasta el *layout* del sistema. Así mismo, KNAPP realiza todas las labores de un centro de distribución ofreciendo soluciones propias, desde tecnología de software hasta el sistema de transporte de mercancía. En nuestro caso nos referimos a toda la maquinaría que existe en cada almacén donde se preparan los pedidos a los socios.

P

PacketShaper: hardware que se encarga de la visualización de la cantidad y del tipo de tráfico que está pasando por la red, permite controlar el tráfico descubierto por la parte de monitorización y establecer prioridades para el uso de las aplicaciones, a parte posee un módulo de compresión que hace que los datos pasados a través del *Packetshaper* sean de menor tamaño y como consecuencia el uso del ancho de banda sea menor, y también tiene un módulo de aceleración que encargará de optimizar las conexiones TCP entre los dos sitios interponiéndose entre los servidores y los clientes y haciendo que las latencias existentes en la red se mitiguen y se pueda llegar a trabajar en la WAN casi como en la LAN. En nuestro caso solo se uso el módulo de monitorización para extraer conclusiones del tráfico de la red en el estado inicial.

Proactivo: el término proactivo refiere a una actitud que puede ser observable en cualquier ser humano y que se caracterizará principalmente entre otras cuestiones por el asumir el control de su vida de modo activo, es decir, lo estático, lo permanente, para una persona que decide como forma de vida adoptar la proactividad no existirá más si es que alguna vez existió, ya que la iniciativa en el desarrollo de acciones marcadas por la audacia y la creatividad serán la manera natural de actuar y comportarse de una persona proactiva/o**.**

R

Rack: Bastidor destinado a alojar equipamiento electrónico, informático y de comunicaciones. Los *racks* son un simple armazón metálico con un ancho interno normalizado de 19 pulgadas, mientras que el alto y el fondo son variables para adaptarse a las distintas necesidades.

Fig. 6.2 Ejemplo de Rack

RRDTool (*Round Robin Database tool*): se trata de una herramienta que trabaja con una base de datos que maneja planificación según Round-Robin. Esta técnica trabaja con una cantidad de datos fija, definida en el momento de crear la base de datos, y un puntero al elemento actual.

S

Sniffer Pro: programa orientado a generar estadísticas de LAN, no directamente a esnifar el contenido del tráfico, si no que nos ayuda a investigar el trafico en sí, que protocolos son los más usados, que trafico hay entre que ordenadores, estadísticas de uso...

Streaming: El termino *streaming* hace referencia a la tecnología de distribución de vídeo o audio a través de Internet. Esta tecnología permite que se almacene en un buffer lo que se va viendo o escuchando sin la necesidad de descargarse el fichero.

STP *(Spaning-Tree-Protocol)*: es un protocolo de red de nivel 2 de la capa OSI. Su función es la de gestionar la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes. El protocolo permite a los dispositivos de interconexión activar o desactivar automáticamente los enlaces de conexión, de forma que se garantice que la topología está libre de bucles. STP es transparente a las estaciones de usuario.

6.3 SQL

En este apartado quiero hacer referencia a algunos SQL que he utilizado para extraer la información de la base de datos de FDF:

SQL usado para el cálculo del número de pedidos

```
select count(*) from gvenpedh
where fecha > "31-12-2007" and fecha <  "01-01-2009"
and tipdoc != "PVV"
```

SQL usado para el cálculo del tiempo de pedido

```
select avg (*) from ff_fedicab_tot

 AVG(((substr(fecha_ok_erp,12,2)*3600 + substr(fecha_ok_erp,15,2)*60 +
substr(fecha_ok_erp,18,2))-
  (substr(fecha_proceso,12,2)*3600  +  substr(fecha_proceso,15,2)*60  +
substr(fecha_proceso,18,2))) -
  ((substr(fecha_ok_socio,12,2)*3600  +  substr(fecha_ok_socio,15,2)*60
+ substr(fecha_ok_socio,18,2))-
   (substr(fecha_proceso,12,2)*3600 + substr(fecha_proceso,15,2)*60 +
substr(fecha_proceso,18,2))
where erp_codter != "S77776" and
fecha > "30-09-2008" and fecha <  "01-01-2009" and
(substr(fecha_ok_erp,12,2)) > 1 and
(EXTEND(fecha_proceso,HOUR     TO     MINUTE))     >     "13:00"     and
(EXTEND(fecha_proceso,HOUR TO MINUTE)) &lt; "15:01"
```